année politique suisse

DOKUMENTATION · ANALYSE · DIFFUSION

Ausgewählte Beiträge zur Schweizer Politik

Suchabfrage	**20.04.2024**
Thema	**Keine Einschränkung**
Schlagworte	**Cyberkriminalität**
Akteure	**Keine Einschränkung**
Prozesstypen	**Keine Einschränkung**
Datum	**01.01.1989 - 01.01.2019**

Impressum

Herausgeber

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

Beiträge von

Ackermann, Nadja
Bühlmann, Marc
Clivaz, Romain
Ehrensperger, Elisabeth
Frick, Karin
Hirter, Hans
Hohl, Sabine
Hulliger, Caroline
Käppeli, Anita
Mosimann, Andrea
Scherrer, Debora
Schmid, Catalina
Schnyder, Sébastien
Schubiger, Maximilian
Schär, Suzanne

Bevorzugte Zitierweise

Ackermann, Nadja; Bühlmann, Marc; Clivaz, Romain; Ehrensperger, Elisabeth; Frick, Karin; Hirter, Hans; Hohl, Sabine; Hulliger, Caroline; Käppeli, Anita; Mosimann, Andrea; Scherrer, Debora; Schmid, Catalina; Schnyder, Sébastien; Schubiger, Maximilian; Schär, Suzanne 2024. ***Ausgewählte Beiträge zur Schweizer Politik: Cyberkriminalität, 1991 - 2018***. Bern: Année Politique Suisse, Institut für Politikwissenschaft, Universität Bern. www.anneepolitique.swiss, abgerufen am 20.04.2024.

Inhaltsverzeichnis

Abkürzungsverzeichnis

EJPD	Eidgenössisches Justiz- und Polizeidepartement
EFD	Eidgenössisches Finanzdepartement
VBS	Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport
UNO	Organisation der Vereinten Nationen
AHV	Alters- und Hinterlassenenversicherung
SECO	Staatssekretariat für Wirtschaft
AB-BA	Aufsichtsbehörde über die Bundesanwaltschaft
SiK-SR	Sicherheitspolitische Kommission des Ständerates
GPK	Die Geschäftsprüfungskommissionen
ETH	Eidgenössische Technische Hochschule
RK-SR	Kommission für Rechtsfragen des Ständerates
SiK-NR	Sicherheitspolitische Kommission des Nationalrates
EU	Europäische Union
MROS	Meldestelle für Geldwäscherei
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
GPDel	Geschäftsprüfungsdelegation
RK MZF	Regierungskonferenz Militär, Zivilschutz und Feuerwehr
SVS	Sicherheitsverbund Schweiz
SISA	Swiss Internet Security Alliance
KMU	Kleine und mittlere Unternehmen
ISB	Informatiksteuerungsorgan des Bundes
MELANI	Melde- und Analysestelle Informationssicherheit
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit
IKT	Informations- und Kommunikationstechnologien
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
SGV	Schweizerischer Gewerbeverband
KOBIK	Schweizerische Koordinationsstelle zur Bekämpfung der Internetkriminalität
AdA	Angehörige(r) der Armee
BWL	Bundesamt für wirtschaftliche Landesversorgung
RS	Rekrutenschule
MERCOSUR	Gemeinsamer Markt des Südens
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NDB	Nachrichtendienst des Bundes (bis 2010: Strategischer Nachrichtendienst und Dienst für Analyse und Prävention)
Fedpol	Bundesamt für Polizei
NSA	National Security Agency: Auslandsgeheimdienst der Vereinigten Staaten

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
ONU	Organisation des Nations unies
AVS	Assurance-vieillesse et survivants
SECO	Secrétariat d'Etat à l'économie
AS-MPC	Autorité de surveillance du Ministère public de la Confédération
CPS-CE	Commission de la politique de sécurité du Conseil des Etats
CdG	Les Commissions de gestion
EPF	École polytechnique fédérale
CAJ-CE	Commission des affaires juridiques du Conseil des Etats
CPS-CN	Commission de la politique de sécurité du Conseil national
UE	Union européenne
MROS	Bureau de communication en matière de blanchiment d'argent
PFPDT	Préposé fédéral à la protection des données et à la transparence
DélCDG	Délégation des Commissions de gestion
CG MPS	Conférence gouvernementale des affaires militaires, de la protection civile et des sapeurs-pompiers

RNS	Réseau national de sécurité
SISA	Swiss Internet Security Alliance
PME	petites et moyennes entreprises
UPIC	Unité de pilotage informatique de la Confédération
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
LMSI	Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure
TIC	Technologies de l'information et de la communication
DFAE	Département fédéral des affaires étrangères
USAM	Union suisse des arts et métiers
SCOCI	Service de coordination de la lutte contre la criminalité sur Internet
Militaire	Militaire
OFAE	Office fédéral pour l'approvisionnement économique du pays
ER	École de recrues
MERCOSUR	Marché commun du Sud
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)
Fedpol	Office fédéral de la police
NSA	National Security Agency: Agence américaine du renseignement extérieur

Allgemeine Chronik

Grundlagen der Staatsordnung

Rechtsordnung

Rechtsordnung

VERWALTUNGSAKT
DATUM: 31.12.1994
HANS HIRTER

Der Vorsteher des EJPD hatte die **innere Sicherheit** zum **Schwerpunktthema** seines Departements für 1994 erklärt. Entsprechend gross fiel denn auch die diesbezügliche Gesetzesproduktion aus. Neben den sich v.a. gegen kriminelle Ausländer ohne Aufenthaltsberechtigung, aber auch gegen abgewiesene Asylbewerber richtenden Zwangsmassnahmen im Ausländerrecht verabschiedete das Parlament die ergänzenden Massnahmen zur Bekämpfung des organisierten Verbrechens und die neuen Strafbestimmungen gegen die Computerkriminalität. Zudem legte der Bundesrat seinen Vorschlag für ein neues Staatsschutzgesetz vor, welches den gesetzlichen Rahmen für die Früherkennung von Spionage, Terrorismus und organisiertem Verbrechen bilden soll. [1]

ANDERES
DATUM: 26.04.2017
MAXIMILIAN SCHUBIGER

Nach der Veröffentlichung der Wirksamkeitsüberprüfung der ersten nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken beschloss der Bundesrat, dass er eine Nachfolgestrategie ausarbeiten möchte. Noch während des letzten Jahres im Zyklus der ersten NCS wurde also die **2. NCS-Strategie** lanciert. Der Schutz vor Cyberkriminalität aller Art sei nach wie vor wichtig, so die Regierung in ihrer Medienorientierung. Vorfälle sowohl in der Schweiz als auch im Ausland zeigten, dass auch kritische Strukturen angegriffen würden und dass Cyber-Angriffe auch für politische Zwecke eingesetzt würden. Die Beurteilung der ersten Strategie 2012–2017 habe gemäss Bundesrat zur Erkenntnis geführt, dass erst ein Fundament habe gelegt werden können, der Schutz jedoch noch ausgebaut werden müsse.
So wurde die Verwaltung beauftragt, eine Nachfolgestrategie für die Jahre 2018 bis 2023 auszuarbeiten, die innert eines Jahres der Regierung unterbreitet werden sollte. Aufbauend auf geschaffenen Strukturen und Prozessen soll der Schutz vor Cyber-Risiken weiter verstärkt werden. Dafür sollen die 30 Stellen weiterhin finanziert und unbefristet verlängert werden. Die Federführung der Arbeiten lag beim ISB. [2]

Äussere Sicherheit

POSTULAT
DATUM: 10.03.2015
KARIN FRICK

Mit einem Postulat wollte die sicherheitspolitische Kommission des Ständerats den Bundesrat beauftragen, in einem Bericht Massnahmen zum **Schutz gegen hybride Bedrohungen** aufzuzeigen, welche über die im Nachrichtendienstgesetz und im BÜPF vorgesehenen hinausgehen. Die beiden hängigen Gesetzesentwürfe werden das rechtliche Instrumentarium diesbezüglich verbessern. In diesem Bereich sind zusätzlich die laufenden Arbeiten zur Umsetzung der Strategie zum Schutz der Schweiz vor Cyberrisiken von grosser Bedeutung. Auch der Bericht zur Sicherheitspolitik 2016 wird das Thema hybride Bedrohungen erörtern. Angesichts der laufenden Arbeiten zum Thema und der in Aussicht stehenden Berichte wurde ein zusätzlicher Bericht, wie ihn das Postulat gefordert hätte, als nicht erforderlich betrachtet. Der Ständerat lehnte das Postulat demzufolge ab. [3]

BERICHT
DATUM: 26.04.2017
MAXIMILIAN SCHUBIGER

Ende April 2017 lag die **Wirksamkeitsüberprüfung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken** wie geplant in Berichtsform vor. Bereits bei der Verabschiedung deren Umsetzungsplans im Jahr 2013 war die Absicht gefasst worden, nach vier Jahren eine Evaluation der NCS vorzunehmen. Dem Bericht konnte entnommen werden, dass die strategische Ausrichtung der NCS richtig gewählt worden war und dass in allen Bereichen funktionierende Prozesse und Strukturen hatten etabliert werden können. Damit könne Spezialwissen gesammelt werden, das die Schweiz besser gegen Cyber-Risiken wappne. Kritisch wurde jedoch auch festgehalten, dass mit der ersten NCS erst quasi ein Fundament gelegt werden konnte, auf dem aufbauend weitere Anstrengungen unternommen werden müssen, um den Schutz im Cyberbereich weiter zu erhöhen.

Im Bericht wurde festgestellt, dass die Schnittstellen zur Armee, also zum Bereich Cyberdefence, noch ungenügend seien. Hier fehle noch eine klarere Abgrenzung und

Zuständigkeit zwischen den zivilen Aufgaben der NCS und der Führung durch die Armee, die für den Konfliktfall noch nicht abschliessend geklärt seien. Im Gegensatz hierzu stehen die Schnittstellen zu den Aktivitäten der Kantone (SVS), denen ein besseres Zeugnis ausgestellt werden konnte und wo die Ziele als erreicht deklariert wurden. Insgesamt wurde unterschieden zwischen einer Beurteilung der genannten Schnittstellen und – im Fokus des Berichts – von einzelnen Massnahmen. Die Wirksamkeitsüberprüfung habe gezeigt, dass die in der Umsetzungsplanung beschriebenen Organisationsstrukturen und Prozesse mehrheitlich implementiert werden konnten und dass verschiedene Produkte (Berichte und Konzepte) termingerecht erstellt worden waren. Dies habe «nachweislich zu gestärkten Kapazitäten, breiterem Wissensstand und besserer Koordination in den verschiedenen Bereichen geführt.» Es war also in der Summe ein durchaus positives Zeugnis, das der externe Evaluator hier der NCS ausgestellt hatte. Es zeichnete sich im Laufe des Frühjahres 2017 dann auch ab, dass der Bundesrat eine zweite Strategie NCS anstrebte. [4]

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 solle 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 solle. 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. [5]

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

Obwaldner weiter.
Verteidigungsminister Parmelin argumentierte vergeblich mit den bestehenden Arbeiten und der Bereitschaft, den Weg der Cyberabwehr weiter gehen zu wollen. Das Ratsplenum nahm die Motion mit 34 zu 7 Stimmen deutlich an. [6]

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) präzisierte 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. [7]

MOTION
DATUM: 12.12.2017
MAXIMILIAN SCHUBIGER

Ein **Cyberdefence-Kommando** innerhalb der Strukturen der Armee zu etablieren, stiess bei der SiK des Nationalrates grundsätzlich auf Zustimmung. Jedoch sahen die Sicherheitspolitikerinnen und -politiker noch Präzisierungspotenzial beim Text der Motion Dittli (fdp, UR). So soll statt von einem Kommando von einer «Cyber-Organisation» die Rede sein. Ferner sei der Begriff «Cyber-Bataillon» unzutreffend, weil dadurch suggeriert werde, dass eine autonome Formation errichtet würde. Hingegen sei vorgesehen, dass IT-Spezialisten der Verwaltung und des Militärs zusammen zum Einsatz kommen würden. Schliesslich wollte die Kommission darauf verzichten, eigens eine Cyber-RS durchzuführen. Stattdessen sollten AdA, die ein Talent im Cyber-Bereich hätten, erst später eine armee(fach)spezifische Cyberausbildung erhalten und in einem weiteren Schritt einer Cyber-Einheit zugeteilt werden. Mit diesen Änderungen gelangte die SiK einstimmig ans Ratsplenum.
In der Nationalratsdebatte folgten nur die nötigsten Wortmeldungen. Kommissionssprecher Dobler (fdp, SG) fasste die zentralen Punkte zusammen. Weil die von der Kommission vorgeschlagenen Änderungen vom Bundesrat angeregt worden waren und in der Kommission Einigkeit geherrscht hatte, konnte der St. Galler auf die Unterstützung seiner Kommissionskolleginnen und -kollegen zählen. Dem Verteidigungsminister blieb nur übrig, die nunmehr von der Regierung mitgetragenen Änderungen zur Annahme zu empfehlen und die Abkehr von der zuvor herrschenden, ablehnenden Meinung bekannt zu geben. In der Folge wurde die Motion im Nationalrat angenommen, wobei sie in der kleinen Kammer aufgrund der vorgenommenen Änderungen nochmals traktandiert werden musste. [8]

POSTULAT
DATUM: 28.02.2018
MAXIMILIAN SCHUBIGER

In der Frühjahrssession 2018 wurde die Debatte eines Postulats, das sich der Thematik **Cyberrisiken** widmete und einen **umfassenden, unabhängigen und wirksamen Schutz** für die Schweiz forderte, aufgenommen. Dabei wurde der Bundesrat von Roger Golay (mcg, GE) aufgefordert, einen Bericht über die Anwendung der Nationalen Strategie gegen Cyberrisiken (NCS) zu erstellen. Man habe, so der Postulant, «nämlich bisher nicht viel [davon] wahrnehmen» können. Der Postulant sorgte sich dabei auch um die Kompetenzenverteilung, so wollte er denn auch beantwortet wissen, wie das

Nebeneinander von EFD und VBS funktioniere und ob dies nicht Risiken berge. Eine Reihe von weiteren Fragen sollte der Bericht auch noch angehen, so beispielsweise wie hochstehendes Fachwissen in der Schweiz erhalten werden kann und wie die Zusammenarbeit zwischen Wissenschaft und Bund intensiviert werden könnte.
Die bundesrätliche Stellungnahme folgte bereits kurz nach der Einreichung und sie war nicht sehr lang, doch hielt die Regierung fest, dass das Postulat Fragen tangiere, die bereits bekannt seien. Sie würden auch in einer Wirksamkeitsprüfung der NCS diskutiert, ein Dokument, das noch im Frühjahr 2017 erscheinen sollte. Eine weitere Analyse, wie die im Postulat geforderte, sei nicht nötig – es wurde also die Ablehnung des Postulats beantragt.
Golay vertrat seinen Vorstoss, der von 62 Nationarlätinnen und Nationalräten mitunterzeichnet worden war, im Parlament. Seiner Meinung nach war sein Postulat nach wie vor aktuell. Der Nationalrat solle auf diesen Bericht beharren: Gerade im Lichte kürzlich zurück liegender Cyber-Attacken auf bundesnahe Betriebe sei diese Form der Aufklärung gerechtfertigt. Bundesrat Maurer versuchte dem Vorstoss noch entgegenzutreten. Man habe sich im Rahmen eines ähnlichen Vorstosses bereits mit dem Thema auseinander gesetzt. Zudem stand eine Klausur des Bundesrats zum Thema Cybersicherheit an, und überhaupt liefen die Arbeiten diesbezüglich auf Hochtouren. Weiter konnte Maurer in Aussicht stellen, dass bereits mit dem Budget 2019 die Anträge zur Schaffung und Stärkung der Cybersicherheit gestellt werden können. Ein Cyber-Securityzentrum wurde mit 40 neuen Stellen veranschlagt, die man über drei Jahre besetzen will. Angesichts aller bereits angestossenen Vorarbeiten könne das Postulat Golay getrost abgelehnt werden. Relativ knapp, mit 100 zu 93 Stimmen (bei drei Enthaltungen) verwarf das Plenum jedoch diesen Antrag und nahm das Postulat an. [9]

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. [10]

MOTION
DATUM: 06.03.2018
MAXIMILIAN SCHUBIGER

In der Frühjahrssession 2018 des Ständerates war die Beschlussfassung zu einem **Cyberdefence-Kommando** nur noch Formsache. Der Motionär selbst, aber auch die ständerätliche SiK, zeigten sich mit der vom Nationalrat veränderten Fassung einverstanden. Weil der Ständerat selbst zuvor bereits einmal dem Anliegen zugestimmt hatte und nun auch in der Ständekammer seitens des Verteidigungsministers grünes Licht gegeben wurde, galt die Motion schon beinahe als angenommen. Ohne Gegenstimme wurde sie denn auch abgesegnet. [11]

POSTULAT
DATUM: 06.03.2018
MAXIMILIAN SCHUBIGER

Angesichts der vielen Vorstösse im Bereich Cyber-Kriminalität und -Abwehr und trotz bereits laufender Projekte (Aktionsplan Cyber-Defence, Nationale Cyber-Strategie) sah die sicherheitpolitische Kommission des Nationalrates in dieser Hinsicht noch Handlungsbedarf. Auch wenn die Arbeiten in der NCS begrüsst würden, brauche es **eine klare Cyber-Gesamtstrategie für den Bund**. Was bisher lanciert wurde, entspreche noch keinem Gesamtkonzept, so die Auffassung der Kommission. Fünf konkrete Aufgaben wurden dem Bundesrat gestellt. Dazu gehörte eine präzise Umschreibung des Auftrags der Armee im Bereich der Cyberverteidigung und des Zuständigkeitsbereichs der zivilen Cyberbehörden. Im Lichte der gewonnenen Erkenntnisse sollte darauf basierend eine Abgrenzung der Kompetenzen vorgenommen und ein entsprechendes Organigramm erstellt werden. Bezüglich Finanzierung sollte man sich ferner Gedanken machen über den Ressourcenbedarf, einschliesslich des Personalbedarfs. Abschliessend wurde vorgeschlagen, dass sich die Schweiz auch am Ausland orientieren möge, wenn es um die Cyberabwehr gehe.
Die Regierung räumte ein, dass längere Zeit unzureichend über dieses Thema nachgedacht und es zeitweise gar unterschätzt worden war. Daher wurde eine solche Gesamtstrategie für unabdingbar erklärt, deutlich unterstützte der Bundesrat also dieses Postulat. Eine «Zerstückelung» des Themas, weil diverse Aktionspläne in unterschiedlichen Departementen erstellt würden, sei nicht wünschenswert.
Im Nationalrat war die Angelegenheit klar, das Postulat wurde angenommen. Kommissionssprecherin Mazzone (gp, GE) und Kommissionssprecher Dobler (fdp, SG) unterstrichen die Wichtigkeit einer koordinierten Vorgehensweise und Dobler äusserte überdies den Eindruck, dass bisher erst wenig geschehen sei, obwohl sich um die 90 Personen in der Bundesverwaltung bereits mit Cyber-Themen befassten. Dies wurde jedoch von Bundesrat Maurer sogleich bestritten. Der Magistrat betonte, dass die Planung weiter fortgeschritten sei, als es vom Vorredner dargestellt worden sei, und er stellte in Aussicht, dass bereits im Budget 2019 erste Positionen für die Umsetzung einer Gesamtstrategie beantragt werden sollten. [12]

ANDERES
DATUM: 18.04.2018
MAXIMILIAN SCHUBIGER

Pünktlich, wie vom Bundesrat gefordert und per Frühling 2018 angekündigt, konnte die **2. NCS verabschiedet** werden. Im April wurde das Papier, das aufzeigt, wie der Bund gemeinsam mit den Kantonen, der Wirtschaft und der Wissenschaft Cyber-Risiken entgegentreten will und welche Handlungsvorgaben für den angestrebten Zeitraum von fünf Jahren gefasst wurden, vom Bundesrat verabschiedet. Aufbauend auf der ersten Umsetzung der NCS wurden sieben Ziele definiert; sie reichen vom Aufbau von Kompetenzen und Wissen bis zu Massnahmen der Cyber-Abwehr, die durch die Armee sichergestellt werden soll. Diese insgesamt 29 Massnahmen wurden in zehn Handlungsfeldern angelegt, wobei auch neue Aspekte abgedeckt werden. So wurde die Verwaltung beauftragt, im Bereich „Standardisierung und Regulierung" aktiv zu werden, um in Kooperation mit der Wirtschaft Mindeststandards für die Cyber-Sicherheit zu etablieren. Ferner sollen sogenannte Cyber-Vorfälle fortan systematisch registriert werden, wofür die Einführung einer Meldepflicht geprüft werden soll. Auch diese Strategie wird in regelmässigen Abständen überprüft, nötigenfalls angepasst und spätestens 2022 aktualisiert. Nur falls es die Bedrohungslage erfordert, wird eine vorzeitige Aktualisierung ins Auge gefasst, nicht jedoch ohne die betroffenen Stellen vorgängig anzuhören. Für die Realisierung und Anwendung der neuen Strategie soll ein Umsetzungsplan erarbeitet werden. Fünf Herausforderungen wurden bereits erkannt: Es braucht zunächst eine klare Verteilung der Verantwortlichkeiten und Kompetenzen innerhalb der Bundesverwaltung. Zweitens muss geprüft werden, ob die geltende Rechtsetzung allenfalls angepasst werden muss, und falls dem so ist, müssen Gesetzesrevisionen über die üblichen Prozesse in die Wege geleitet werden, was unter Umständen viel Zeit in Anspruch nehmen kann. Als drittes gilt es, die Zusammenarbeit mit den Partnern aus der Wirtschaft und den Hochschulen, aber auch den Kantonen, zu definieren. Viertens braucht es messbare Leistungsziele, um den Umsetzungsfortschritt der Strategie nachvollziehen und transparent beurteilen zu können. Die allfällige vorzeitige Aktualisierung bedarf, fünftens, klarer Vorgaben und Kriterien: Die Umstände

für eine Anpassung müssen ebenso wie die Verantwortlichkeiten festgelegt werden. [13]

VERWALTUNGSAKT
DATUM: 27.08.2018
MAXIMILIAN SCHUBIGER

Ende August 2018 gelangte das BWL infolge einer Verwundbarkeitsanalyse zu Cyberrisiken mit Empfehlungen, den sogenannten **IKT-Minimalstandards**, an die Öffentlichkeit. Dabei standen lebenswichtige Branchen im Zentrum des Interesses, namentlich die Stromversorgung, Trinkwasser- und Lebensmittelversorgung sowie auch der Strassen- und Schienenverkehr. Besonders Betreiber von kritischen Infrastrukturen sollen sich an diese Mindeststandards («IKT-Resilienz») halten, sie seien jedoch für alle Unternehmen anwendbar. Über 100 konkrete Handlungsanweisungen in den Bereichen Identifizieren, Schützen, Detektieren, Reagieren und Wiederherstellen waren zuhanden der Betreiber ausgearbeitet worden. In Kooperation mit dem Verband Schweizerischer Elektrizitätsunternehmen sei bereits ein Standard für die Strombranche erarbeitet worden. Dieser Schritt war im Zuge der 2012 vom Bundesrat lancierten Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) unternommen worden. [14]

MOTION
DATUM: 10.09.2018
MAXIMILIAN SCHUBIGER

Die Motion Grüter (svp, LU) beschäftigte im Sommer die ständerätliche SiK. Der **Ausbau der Cyberabwehrkompetenzen** wurde vom Gremium mehrheitlich begrüsst, gleichwohl überwogen Bedenken bezüglich der Motion. Die SiK-SR schlug deswegen ihrem Rat vor, die Motion nicht anzunehmen. Man wollte sich mit diesem Schritt Zeit verschaffen, um bereits in Angriff genommene Projekte weiterzuführen. Namentlich ging es um die beiden überwiesenen Motionen zu einem Cyberdefence-Kommando in der Armee und zu einem Cybersecurity-Kompetenzzentrum. Diese laufenden Massnahmen wurden von der SiK begrüsst, wohingegen die vorliegende Motion widersprüchliche Folgen zu bereits getätigten Beschlüssen hätte. Besonders die angeregte Zentralisierung der Cyberkompetenzen an einer Amtsstelle (innerhalb des VBS) wurde von den Kommissionsangehörigen mehrheitlich abgelehnt. Man vergebe sich dadurch viele bereits erlangte Kenntnisse und die bisherigen Mechanismen innerhalb des EFD und MELANI funktionierten gut. Aus ordnungspolitischer Sicht wurde die Motion zudem abgelehnt, weil es der Regierung und nicht dem Parlament obliege, federführende Stellen innerhalb der Verwaltung zu bestimmen. Diesem Antrag stimmten 10 Kommissionsmitglieder zu, zwei waren dagegen.
Dieser deutlichen Kommissionsmeinung folgte dann auch das Ratsplenum, das die Motion ablehnte und damit den recht deutlichen Beschluss des Erstrates umstiess. Kommissionssprecher Dittli (fdp, UR) und Bundesrat Maurer waren die Einzigen, die sich zu Wort meldeten. Beide betonten die bereits angestossenen Arbeiten und die guten Fortschritte im Cybersicherheitsbereich. Die Regierung erkenne im Vorschlag Grüter keine bessere Lösung, erklärte Maurer. Oppositionslos wurde das Geschäft verworfen. [15]

Rechtshilfe

MOTION
DATUM: 03.12.2018
KARIN FRICK

Mit einer im März 2018 eingereichten Motion verfolgte die RK-SR zwei Ziele: Erstens sollen soziale Netzwerke rechtlich dazu verpflichtet werden, als Ansprechpartner für die schweizerischen Behörden sowie zur einfacheren Einreichung von Beanstandungen durch die Nutzerinnen und Nutzer eine Vertretung oder ein Zustelldomizil in der Schweiz einzurichten. Zweitens soll die Schweiz auf internationaler Ebene aktiv werden, um eine Lösung für das Problem der **Rechtsdurchsetzung im Internet** zu finden. Wie es der Bundesrat beantragt hatte, stimmten im Mai bzw. Dezember 2018 beide Räte dem Vorstoss stillschweigend zu. [16]

Datenschutz und Statistik

PARLAMENTARISCHE INITIATIVE
DATUM: 29.05.2012
NADJA ACKERMANN

Eine von Nationalrat Hochreutener (cvp, BE) eingereichte parlamentarische Initiative forderte, dass Hostingprovider für unzureichenden **Schutz der von ihnen gespeicherten Informationen** zur Verantwortung gezogen werden können. Die Rechtskommission des Nationalrates empfahl die Initiative nach der Ablehnung ihrer Schwesterkommission nun ebenfalls zur Ablehnung, weil seit dem Einreichen der Initiative verschiedene gesetzliche wie auch nichtgesetzgeberische Massnahmen ergriffen worden waren. Der Nationalrat folgte dem Antrag seiner Kommission in der Sommersession 2012. [17]

ANDERES
DATUM: 11.04.2014
NADJA ACKERMANN

Im April 2014 sorgte die Aufdeckung einer **Sicherheitslücke bei der weitverbreiteten Verschlüsselungssoftware Open SSL** für Aufregung. Durch das „**Heartbleed**" genannte Leck konnten Kriminelle an sensible Daten wie Passwörter gelangen. Betroffen waren viele Dienstleistungsanbieter wie Krankenversicherer, Banken, Webshops, Google und Yahoo. Nachdem die Sicherheitslücke wohl zwei Jahre bestanden hatte, konnte sie bei den betroffenen Banken in der Schweiz innerhalb eines Tages geschlossen werden. [18]

PARLAMENTARISCHE INITIATIVE
DATUM: 29.08.2014
NADJA ACKERMANN

Snowden, fortschreitende Digitalisierung, NSA-Skandale und Cyber-Crimes rückten den Datenschutz zuoberst auf die Politikagenda und verhalfen der Datenschutzproblematik zu einer hohen Medienpräsenz. Die zunehmende Angst vor dem „gläsernen Bürger" erhielt daher in Gestalt verschiedener Vorstösse auch Einzug ins Parlament. Unter ihnen befand sich eine parlamentarische Initiative Vischer (gp, ZH), welche ein **Grundrecht auf informationelle Selbstbestimmung** verankern wollte. Die moderne Datenverarbeitung gefährde nicht nur die freie Entfaltung der Persönlichkeit, sondern durch die selbstbestimmte Mitwirkung der Bürger auch das Gemeinwohl. Aus diesem Grund soll der verfassungsrechtliche Datenschutz von einem Missbrauchsschutz zu einem Grundrecht auf informationelle Selbstbestimmung aufgewertet werden. Damit würde ein Paradigmenwechsel in der Beweislast zugunsten der Bürger und Bürgerinnen vorgenommen. Die sicherheitspolitische Kommission des Nationalrates gab dem Vorstoss mit 12 zu 8 Stimmen Folge. [19]

Grundrechte

MOTION
DATUM: 05.03.2014
NADJA ACKERMANN

Mit einer Motion Schmid-Federer (cvp, ZH) möchte der Nationalrat den Bundesrat beauftragen, eine **nationale Strategie gegen Cyberbullying und Cybermobbing** auszuarbeiten. Die Strategie sollte mindestens eine national koordinierte Bekämpfung, eine zentrale Anlaufstelle für Opfer und Eltern sowie eine breit angelegte nationale Aufklärungskampagne umfassen. Der Bundesrat sah jedoch aufgrund der 2010 lancierten Programme „Jugend und Gewalt" und „Jugend und Medien" keinen Handlungsbedarf. Der Ständerat äusserte sich im Berichtsjahr noch nicht zum Anliegen. [20]

MOTION
DATUM: 08.09.2015
KARIN FRICK

Eine Motion Schmid-Federer (cvp, ZH) zur Ausarbeitung einer **nationalen Strategie gegen Cyberbullying und Cybermobbing** wurde von der kleinen Kammer in der Herbstsession 2015 abgelehnt. Im Vorjahr war der Vorstoss im Nationalrat überwiegend auf Unterstützung gestossen. Der Ständerat folgte mit dem Entscheid den Anträgen des Bundesrates und seiner Kommission für Wissenschaft, Bildung und Kultur. Vor dem Hintergrund der erfolgreichen Förder- und Präventionsmassnahmen im Rahmen der beiden nationalen Programme «Jugend und Medien» sowie «Jugend und Gewalt» sei der Nutzen der geforderten nationalen Strategie grundsätzlich in Frage zu stellen. Ein weiterer Kritikpunkt war die angezweifelte Effektivität der zentralen Anlaufstelle; die Zuständigkeit wurde hier primär bei den Kantonen gesehen. [21]

Innere Sicherheit

INTERNATIONALE BEZIEHUNGEN
DATUM: 20.03.2008
HANS HIRTER

Der Nationalrat überwies diskussionslos eine Motion Glanzmann (cvp, LU) für eine rasche Unterzeichnung der **Cybercrime-Konvention des Europarates**. Diese vereinfacht die internationale Rechtshilfe bei der Ermittlung von Verbrechen, die im Internet begangen worden sind. Der Ständerat überwies eine Motion Burkhalter (fdp, NE; Mo. 08.3100) und ein Postulat Frick (cvp, SZ; Po. 08.3101), welche einen Bericht über die effizientesten Möglichkeiten zur Bekämpfung der Internetkriminalität und darauf aufbauend eine nationale Strategie dazu fordern. [22]

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. [23]

MOTION
DATUM: 15.03.2011
NADJA ACKERMANN

In diesem Sinne unterstützte der Bundesrat auch eine allgemeingefasste Motion der sicherheitspolitischen Kommission des Nationalrates, die die Regierung beauftragt, eine gesetzliche Grundlage für die **Sicherung und Verteidigung wichtiger Schweizer Datennetzwerke** zu schaffen. Nachdem die Motion von der grossen Kammer 2010 überwiesen worden war, folgte nun auch der Ständerat dem Antrag seiner Kommissionsmehrheit und nahm die Motion an. [24]

POSTULAT
DATUM: 18.03.2011
NADJA ACKERMANN

Für die Eindämmung der Gefahren, die vom Internet ausgehen, sprach sich auch der Nationalrat aus. So hiess er ein Postulat Darbellay (cvp, VS) gut, welches den Bundesrat beauftragt, ein Konzept zum **Schutz der digitalen Infrastruktur** der Schweiz vorzulegen. In seiner Stellungnahme erklärte der Bundesrat, dass er sich der Bedeutung von Cyber-Bedrohungen bewusst sei und er deshalb beschlossen habe, die Federführung für das Thema Cyber Defense auf Stufe Bund dem VBS zu übertragen. Am 10. Dezember 2010 war für eine befristete Zeit ein Projektleiter in der Person von Divisionär Kurt Nydegger gewählt worden. Ein Strategiepapier zur Cyber Defense soll im Frühling 2012 vorliegen. Im Verlaufe des Jahres zeigte sich, dass Ueli Maurer und seine Spezialisten eine Kooperation mit dem Nato Cooperative Cyber Defence Centre in der estnischen Hauptstadt Tallinn anstreben. [25]

POSTULAT
DATUM: 18.03.2011
NADJA ACKERMANN

Konkreter war ein Postulat der FDP-Liberale-Fraktion, welches die Schaffung einer Leit- und Koordinationsstelle für die präventive Gefahrenabwehr im Bereich **Cyber-Bedrohung** vorsieht und vom Nationalrat überwiesen wurde. [26]

VERWALTUNGSAKT
DATUM: 30.05.2012
NADJA ACKERMANN

Für grosse Aufruhr sorgte ein **Spionagefall im Nachrichtendienst**. Ein beim Nachrichtendienst des Bundes angestellter Informatik-Spezialist hatte eine Datenmenge im Tera-Bereich gestohlen. Aufgrund von Hinweisen der UBS konnte der Dieb verhaftet und die Daten sichergestellt werden, bevor sie wie geplant ins Ausland verkauft werden konnten. Durch den Datendiebstahl wurde auch das sich in Ausarbeitung befindende, neue Nachrichtendienstgesetz aktuell. Dieses sieht u.a. die Schaffung einer gesetzlichen Grundlage vor, mit welcher der Nachrichtendienst seine Agenten jederzeit überprüfen kann. Auch die Geschäftsprüfungsdelegation des Parlaments beschäftigte sich mit dem Spionagefall und will bis Frühling 2013 einen Bericht zuhanden des Bundesrates abschliessen. [27]

VERWALTUNGSAKT
DATUM: 27.06.2012
NADJA ACKERMANN

Der Bundesrat verabschiedete am 27. Juni 2012 eine auch durch verschiedene parlamentarische Vorstösse geforderte **nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken**. Die Strategie sieht vor, dass die bestehende Zusammenarbeit mit Behörden, Wirtschaft und den Betreibern kritischer Infrastrukturen vertieft wird. Zwar soll zusätzlich zur Melde- und Analysestelle Informationssicherung (MELANI) eine Koordinationsstelle im EFD geschaffen werden, jedoch verzichtet die Regierung auf ein zentrales Steuerungs- und Koordinationsorgan. Die Verantwortung liegt weiterhin bei den Organisationseinheiten, während der Staat nur subsidiäre Aufgaben wie Informationsaustausch und nachrichtendienstliche Erkenntnisse übernimmt. [28]

VERWALTUNGSAKT
DATUM: 15.05.2013
NADJA ACKERMANN

Im Mai 2013 verabschiedete der Bundesrat einen Umsetzungsplan für die im Vorjahr vorgelegte **Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken** (NCS). Der bis 2017 laufende **Umsetzungsplan** konkretisiert sechzehn Massnahmen der Strategie und legt die Verantwortlichkeiten fest. Da eine personelle Verstärkung im Fachbereich Cyber nötig ist, beabsichtigte der Bundesrat die Schaffung von 28 Stellen in diesem Bereich. [29]

BERICHT
DATUM: 03.07.2013
NADJA ACKERMANN

Dass Handlungsbedarf bezüglich des Nachrichtendienstes besteht, hat im vergangen Jahr der **Spionagefall im Nachrichtendienst des Bundes (NDB)** bestätigt. Im Nachgang an den durch einen UBS-Mitarbeiter aufgedeckten Datendiebstahl beim NDB im Mai 2012 führte die Geschäftsprüfungsdelegation (GPDel) vom November 2012 bis Februar 2013 eine formelle Inspektion zur Informatiksicherheit im NBD durch. Im Juli 2013 übergab die Delegation den Bericht sowie elf Empfehlungen an den Bundesrat. Der Öffentlichkeit wurde aus Überlegungen zum Schutz des Staatsinteresses lediglich eine Zusammenfassung des Berichts zugänglich gemacht. Die GPDel hatte festgestellt, dass bei der Schaffung des NDB aus den beiden Vorgängerorganisationen ein Defizit an Personalressourcen bestand, da das VBS den Dienst für Analyse und Prävention (DAP) ohne Personal vom EJPD übernommen hatte. Der NBD hatte folglich dasselbe Aufgabenpensum mit weniger Arbeitskräften zu bewältigen. Aufgrund dieser knappen Personalressourcen in der Informatik und des unzulänglichen Risikomanagements war der NBD zu wenig darauf ausgerichtet, die Verfügbarkeit, die Integrität und die Vertraulichkeit der Daten als zentrale Zielsetzung der Informatiksicherheit zu gewährleisten. [30]

MOTION
DATUM: 03.06.2014
NADJA ACKERMANN

Erneute Spionageskandale hatten die Sicherheitspolitische Kommission des Nationalrates (SiK-NR) dazu bewogen, mit einer Motion die Umsetzung der nationalen **Strategie zum Schutz der Schweiz vor Cyberrisiken** bereits bis Ende 2016 statt wie vorgesehen 2017 zu fordern. Während der Nationalrat diesem Anliegen zugestimmt hatte, lehnte die kleine Kammer selbiges mit 17 zu 16 Stimmen mit dem Argument ab, dass eine Fristverkürzung sowohl Qualitätseinbussen als auch Finanzierungsprobleme mit sich bringen würde. [31]

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. [32]

ANDERES
DATUM: 04.05.2017
MAXIMILIAN SCHUBIGER

Der **Sicherheitsverbund Schweiz** (SVS) hat im ersten Halbjahr 2017 **zwei Veranstaltungen** durchgeführt. Anfang April fand zum fünften Mal die Cyber-Landsgemeinde statt. In Bern trafen sich etwa 100 Vertrererinnen und Vertreter von Bund und Kantonen, um über die NCS zu diskutieren. Im Fokus standen dabei die Cyberkriminalität und Cybersicherheit.

Die NCS stand auch bei der dritten Konferenz des SVS im Zentrum der Aufmerksamkeit. Rund 400 Personen waren für diesen Anlass zusammengekommen, bei dem ebenfalls der Schutz vor Cyberrisiken sowie die Sicherheit im Cyberbereich thematisiert wurden. Da die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken Ende 2017 auslief, stellte sich die Frage nach der künftigen Ausgestaltung der Cyber-Abwehr. Der Verteidigungsminister hatte dabei Gelegenheit, die neue Cyberverteidigungsstrategie vorzustellen, die das VBS erarbeitete. [33]

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. [34]

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. [35]

ANDERES
DATUM: 26.04.2018
MAXIMILIAN SCHUBIGER

2018 fand die **sechste Cyber-Landsgemeinde des Sicherheitsverbundes Schweiz** statt. Die Nachfolgearbeiten der ersten NCS standen dabei im Zentrum: Im Zuge der Aufarbeitung der 16 Massnahmen aus der ersten Strategie wurde den Teilnehmenden aus Bund, Kantonen und der Privatwirtschaft aufgezeigt, welche Themen für die NCS II relevant sein werden; gleichzeitig wurden sie in die Erarbeitung dieser Nachfolgestrategie involviert. Weitere Themen waren die Entwicklung und Einführung von Minimalstandards im IKT-Bereich, neue Arten der Cyberkriminalität und die Schwierigkeiten, diese zu erkennen und zu bekämpfen, die Reduktion von IKT-Verwundbarkeiten und, damit zusammenhängend, eine verbesserte Resilienz. Als Herausforderung galten ferner auch die Bedeutung einer korrekten Erkennung und Einschätzung der Bedrohungen aus dem Cyberraum und die geeignete Handhabung dieser Gefährdung. [36]

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. [37]

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. [38]

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. [39]

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. [40]

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. [41]

ANDERES
DATUM: 07.10.1994
HANS HIRTER

Die 1991 vom Bundesrat beantragte **Strafrechtsrevision** in bezug auf strafbare Handlungen gegen das Vermögen und auf Urkundenfälschung konnte **abgeschlossen** werden. In der Differenzbereinigung schloss sich der Nationalrat weitgehend den Entscheiden der kleinen Kammer an. [42]

MOTION
DATUM: 18.12.1998
HANS HIRTER

Bei **strafbaren Handlungen im Internet** (z.B. Angebot von illegaler Pornographie und Verbreitung von gegen das Antirassismusgesetz verstossenden Aussagen) bestehen nicht nur Probleme bei der Verfolgung der Täter, da diese ja oft in Staaten tätig sind, wo ihre Aktionen nicht verboten sind (z.B. rassistische Aussagen in den USA). Unklarheit besteht auch in bezug auf die **rechtliche Mitverantwortung der sogenannten Provider**, die als Vermittler zwischen den Internetnutzern fungieren. Gemäss dem seit April 1998 geltenden neuen Medienstrafrecht können diese wegen Nichtverhinderung einer strafbaren Publikation zur Verantwortung gezogen werden, wenn es nicht möglich ist, die Autoren selbst in der Schweiz zu belangen. Der Bundesrat beantragte dem Nationalrat erfolgreich die Umwandlung einer Motion von Felten (sp, BS) für einen spezifischen Strafrechtsartikel, der die Verantwortlichkeit der Provider festhält, in ein Postulat. Er riet dabei, die weitere Entwicklung abzuwarten, da sich das Problem ohnehin nur auf internationaler Ebene lösen lasse und zudem auch die Provider selbst versuchten, Standards für eine Selbstregulierung zu entwickeln. Im Juli hatte die Bundesanwaltschaft einige Provider ersucht, für ihre Abonnenten den Zugang zu Seiten mit in der Schweiz illegalen Inhalten zu sperren. Die Provider wiesen in ihrer Reaktion auf die technischen Probleme solcher Sperren hin, bei denen entweder Tausende von legalen Seiten gleichzeitig gesperrt würden, oder die nutzlos blieben, da die Autoren in kürzester Zeit unter neuen Adressen auftauchen würden. [43]

MOTION
DATUM: 20.09.2001
HANS HIRTER

Zusätzlicher strafrechtlicher Regelungsbedarf besteht weiterhin auf dem Gebiet der sogenannten **Internetkriminalität**. Sowohl bei der Übermittlung unerlaubter Darstellungen und Meinungsäusserungen (z.B. Gewalt, verbotene Pornografie, rassistisches Gedankengut) als auch bei der Vermittlung von illegalen Geschäften (z.B. Kinderhandel) bestand bisher rechtliche Unsicherheit über die Strafbarkeit des sog. Access-Providers, also der Firma, welche den einzelnen Nutzern den Zugang zum Internet ermöglicht. Die Frage nach deren rechtlicher Verantwortlichkeit ist insbesondere auch deshalb von Bedeutung, weil sich die Inhaber von Internetseiten mit in der Schweiz verbotenen Darstellungen und Angeboten meist nicht in der Schweiz selbst befinden. Das Parlament überwies eine Motion Pfisterer (fdp, AG), welche in allgemeiner Form eine international harmonisierte Regelung fordert. Der Nationalrat hiess zudem eine Motion Aeppli (sp, ZH) gut, welche eine Zentralisierung der Ermittlungen im Bereich der sexuellen Ausbeutung von Kindern im Internet beim Bund fordert. [44]

MOTION
DATUM: 09.06.2006
HANS HIRTER

Mit der Überweisung einer Motion Schweiger (fdp, ZG) sprach sich der Ständerat für die Verschärfung der strafgesetzlichen Bestimmungen im Kampf gegen verbotene **pornografische Darstellungen im Internet** (v.a. Kinderpornografie) aus. Der Vorstoss fordert insbesondere, dass nicht nur der Besitz derartiger Filme und Bilder verboten ist, sondern bereits der absichtliche Konsum. Um die Strafverfolgung zu erleichtern, soll zudem die Aufbewahrungspflicht für die Logbuchdateien der Internetanbieter von sechs auf zwölf Monate verlängert werden. Der Nationalrat behandelte diese Motion noch nicht, stimmte aber einer Motion Hochreutener (cvp, BE; Mo. 06.3554) zu, welche verlangt, dass dieselben Mittel auch im Kampf gegen extreme Gewaltdarstellungen zur Anwendung kommen. [45]

MOTION
DATUM: 11.12.2007
HANS HIRTER

Der Nationalrat überwies die Motion von Ständerat Schweiger (fdp, ZG; Mo. 06.3170) für eine Verschärfung der strafgesetzlichen Bestimmungen im Kampf gegen verbotene **pornografische Darstellungen im Internet** (v.a. Kinderpornografie). Der Ständerat seinerseits nahm die Ende 2006 von Nationalrat überwiesene Motion Hochreutener (cvp, BE; Mo. 06.3554) an, welche verlangt, dass dieselben Mittel auch im Kampf gegen extreme Gewaltdarstellungen zur Anwendung kommen sollen. [46]

MOTION
DATUM: 03.03.2011
NADJA ACKERMANN

In die vom Bundesrat geforderte Richtung der **Sensibilisierung von Jugendlichen im Umgang mit den neuen Medien** ging eine Motion Schweiger (fdp, ZG), die im Lehrplan 21 einen Medienführerschein einbauen wollte. Nachdem sie letztes Jahr vom Ständerat angenommen wurde, lehnte sie der Nationalrat aber ab. [47]

MOTION
DATUM: 03.03.2011
NADJA ACKERMANN

Nach dem Ständerat überwies auch der Nationalrat eine Motion Bischofberger (cvp, AI), die den Bundesrat beauftragt, eine gesetzliche Grundlage zu schaffen, um eine effizientere und kostengünstigere Zusammenarbeit der im Bereich **Jugendmedienschutz** und Bekämpfung von Internetkriminalität tätigen Organe des Bundes sicherzustellen und Doppelspurigkeiten zu vermeiden. [48]

INTERNATIONALE BEZIEHUNGEN
DATUM: 18.03.2011
NADJA ACKERMANN

Da das Internet keine Landesgrenzen kennt, ist bei der Bekämpfung der Internetkriminalität eine internationale Zusammenarbeit wichtig. Dieser Ansicht ist auch die grosse Kammer, die nach dem Ständerat ebenfalls den Entwurf des Bundesrates zur Umsetzung des **Übereinkommens des Europarates über die Cyberkriminalität** mit 117 zu 30 Stimmen genehmigte. Nur die SVP votierte gegen die Konvention. Zu Diskussionen führte der von der Schweiz anzubringende Vorbehalt, mit dem bei Pornografie auf dem Schutzalter 16 statt 18 beharrt werden soll. Durch die Ratifizierung der Konvention wird der Straftatbestand um das Hacking erweitert. Zugleich wurde so der Motion Glanzmann-Hunkeler (cvp, LU; Mo. 07.3629) Folge geleistet, welche bereits 2007 die rasche Unterzeichnung der Konvention gefordert hatte. [49]

PARLAMENTARISCHE INITIATIVE
DATUM: 19.05.2011
NADJA ACKERMANN

Die letztes Jahr eingereichte parlamentarische Initiative Schmid-Federer (cvp, ZH), welche die **Effektivität und Effizienz in den Bereichen Jugendmedienschutz und Internetkriminalität** sicherstellen wollte, wurde im Mai von der Initiantin zurückgezogen. [50]

MOTION
DATUM: 20.09.2011
NADJA ACKERMANN

Das Parlament überwies eine Motion Amherd (cvp, VS), die den Bundesrat beauftragt, an der im Januar 2012 tagenden, intergouvernementalen Expertengruppe der UNO zu Cyber Crime die Bekämpfung des **virtuellen Kindesmissbrauchs** zu thematisieren. [51]

MOTION
DATUM: 20.09.2011
NADJA ACKERMANN

Um die bessere Verfolgung von Pädophilen zu ermöglichen, sollen Internetanbieter verpflichtet werden, die Protokolle über die **Zuteilung von IP-Adressen**, die Kundinnen und Kunden zur Verfügung gestellt werden, mindestens ein ganzes statt wie bisher ein halbes Jahr aufzubewahren. Dies fordert eine von beiden Kammern überwiesene Motion Barthassat (cvp, GE). [52]

GESELLSCHAFTLICHE DEBATTE
DATUM: 20.03.2014
NADJA ACKERMANN

Im Rahmen der Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) auf Stufe der Kantone und der Gemeinden fand im März 2014 in Bern die **zweite Cyber-Landsgemeinde** statt. Ziel des durch den Sicherheitsverbund Schweiz (SVS) organisierten Anlasses war der Austausch über den Umsetzungsstand der Strategie sowie die Koordination des weiteren Vorgehens. Die nächste Cyber-Landsgemeinde soll 2015 stattfinden. [53]

ANDERES
DATUM: 08.05.2014
NADJA ACKERMANN

Trotz eines leichten Rückgangs war auch im Jahr 2013 die Anzahl der gemeldeten, verdächtigen Vermögenswerte hoch. Ihr Umfang belief sich auf knapp drei Milliarden CHF, wobei insgesamt 30 Verdachtsmeldungen Summen von über 10 Millionen CHF betrafen. Meist handelte es sich bei der mutmasslich begangenen Vortat zur **Geldwäscherei** um Betrug, wobei eine Zunahme von Computerbetrugsfällen verzeichnet wurde. Die Abnahme der Fälle erlaubte eine vertiefte Analyse der eingegangenen Verdachtsmeldungen und raschere und besser fundierte Meldungen an die Strafverfolgungsbehörden. Dies hielt der im Mai 2014 veröffentlichte Jahresbericht der Meldestelle für Geldwäscherei (MROS) fest. [54]

ANDERES
DATUM: 11.09.2014
NADJA ACKERMANN

Im September 2014 gründeten Vertreter der Wirtschaft die branchenübergreifende **Swiss Internet Security Alliance** (SISA), um die Sicherheit von Schweizer Online-Angeboten auch in Zukunft zu gewährleisten. Der Verein, dem unter anderem Swisscom, UBS, Switch und PostFinance angehören, folgt dem Ruf nach einer verstärkten Zusammenarbeit bei der Bekämpfung der Internetkriminalität. Zu diesem Zweck bietet SISA einen kostenlosen Swiss Security Check an, der Problemstellen aufdecken soll. [55]

GESELLSCHAFTLICHE DEBATTE
DATUM: 20.11.2014
NADJA ACKERMANN

Am 20. November 2014 fand in Bern die vom Informatiksteuerungsorgan des Bundes (ISB) organisierte Tagung zum Thema **Cyber-Risiken Schweiz** statt. Die rund 150 Teilnehmer aus Bund, Kantonen und Wirtschaft diskutierten an verschiedenen Podien über den aktuellen und zukünftigen Schutz kritischer Infrastrukturen in der Schweiz. Offen blieb dabei die Frage, wem die Hauptverantwortlichkeit beim Schutz vor Cyber-Angriffen zufällt. Es bestand jedoch Konsens darüber, dass ein effektiver Schutz nur in intra- und internationaler Zusammenarbeit gewährleistet werden könne. [56]

POSTULAT
DATUM: 30.09.2016
KARIN FRICK

Die meisten Hackerangriffe auf Daten sammelnde und lagernde Organisationen werden aus Angst vor Imageschäden verschwiegen. Mit der stillschweigenden Annahme eines Postulats Béglé (cvp, VD) trug der Nationalrat dem Bundesrat auf zu prüfen, ob und wie solche Organisationen verpflichtet werden können, **nach Hackerangriffen die geschädigten Personen über den Vorfall zu informieren**. Personen, deren elektronische Daten durch den Angriff in die Hände Dritter gelangt sind, soll mit dieser Informationspflicht die Möglichkeit gegeben werden, etwas zu unternehmen, um den Schaden zu begrenzen. Darüber hinaus sollte die Aussicht auf einen Imageschaden Organisationen in Verantwortung für elektronische Daten wachsamer werden lassen. [57]

MOTION
DATUM: 29.09.2017
KARIN FRICK

Vor dem Hintergrund der wachsenden Bedrohung durch Cyberkriminalität forderte eine im Sommer 2017 eingereichte Motion Dobler (fdp, SG) die **Schaffung einer zentralen Anlauf- und Koordinationsstelle zur Bekämpfung der organisierten und international tätigen Computerkriminalität**. Der zunehmenden Komplexität und Vielschichtigkeit dieser Art von Bedrohung sei die föderal fragmentierte Strafverfolgung in der Schweiz nicht gewachsen, weshalb es einer zentralen Anlaufstelle beim Bund bedürfe, um die Zusammenarbeit in der Strafverfolgung operativ zu koordinieren, so die Begründung des Motionärs. Dem Antrag des Bundesrates folgend, stimmte der Nationalrat in der Herbstsession 2017 dem Vorstoss stillschweigend zu. [58]

MOTION
DATUM: 14.03.2018
CATALINA SCHMID

Nach der einstimmigen Annahme im Nationalrat kam die Motion Dobler (fdp, SG), welche eine **zentrale Anlauf- und Koordinationsstelle zur Bekämpfung der organisierten und international tätigen Computerkriminalität** forderte, im Frühjahr 2018 zur Behandlung in den **Ständerat**. Die Bekämpfung der immer grösser werdenden Herausforderung der digitalen Kriminalität verlange eine stärkere Zentralisierung und Koordinierung bei der Beweiserhebung und -sicherung, begründete die RK-SR ihren einstimmigen Antrag auf Annahme. Wie Justizministerin Simonetta Sommaruga im Rat zustimmend anfügte, betreffe eine solche Anlauf- und Koordinationsstelle sowohl den Bund als auch die Kantone. Aus diesem Grund sei es sinnvoll, diese Zusammenarbeit gesetzlich zu verankern. Im Rahmen des Bundesgesetzes über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (PMT), welches bereits in Vernehmlassung sei, sei eine gesetzliche Grundlage für die Bekämpfung der digitalen Kriminalität zudem vorgesehen. Diese Stossrichtung werde durch die Motion Dobler bestärkt; aus diesem Grund beantrage auch der Bundesrat deren Annahme. Der Ständerat folgte diesen Empfehlungen und nahm die Motion stillschweigend an. [59]

POSTULAT
DATUM: 16.03.2018
KARIN FRICK

Mit der stillschweigenden Überweisung eines Postulats Glättli (gp, ZH) forderte der Nationalrat in der Frühjahrssession 2018 den Bundesrat auf, **Sicherheitsstandards für Internet-of-Things-Geräte zu prüfen**. In der Begründung des Vorstosses identifizierte der Postulant die ans Internet angebundenen Geräte (sogenanntes Internet of Things) als eine der grössten Bedrohungen für die Cybersicherheit in der Schweiz, weil sie bei der Einfuhr zwar Elektronik- und Funkstandards, nicht aber einfachste Grundsätze der Informationssicherheit erfüllen müssten. Der Bundesrat hatte die Annahme des Postulats beantragt, weil er es als sinnvoll erachtete, die im Vorstoss aufgeworfenen Fragen zu untersuchen. [60]

Institutionen und Volksrechte

Regierungspolitik

ANDERES
DATUM: 14.11.2018
MARC BÜHLMANN

Auch **2018** trafen sich die Partei- und Fraktionsspitzen der Regierungsparteien mit Vertretungen der Landesregierung zu den **Von-Wattenwyl-Gesprächen**. Die Gespräche finden seit Jahren jeweils vor den Parlamentssessionen statt und sollen informelle Diskussionen zu wichtigen aktuellen politischen Themen erlauben.
Anfang Februar tauschten sich die Präsidien der Regierungsparteien mit dem Bundespräsidenten Alain Berset, mit Bundesrätin Doris Leuthard und Bundesrat Ignazio Cassis sowie Bundeskanzler Walter Thurnherr über den Strommarkt und die Europapolitik aus. Im Zentrum der Diskussion standen dabei die im Rahmen der Revision des Stromversorgungsgesetzes anvisierte Planung der Versorgungssicherheit mit Strom sowie die geplanten Schritte zu den Beziehungen mit der EU. Intensive Debatten habe es zur Frage der dynamischen Rechtsübernahme bei einem allfälligen Rahmenabkommen gegeben, liess sich der Medienmitteilung entnehmen.
Bei den Gesprächen vor der Frühlingsession wurde der Bundespräsident von Bundesrat Ueli Maurer und erneut vom Bundeskanzler begleitet. Thema war die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS), deren Verantwortung beim EFD lag. Die Gesprächsteilnehmenden waren sich einig, dass es hier Zusammenarbeit zwischen allen Departementen und in den Bereichen Cyber-Sicherheit, Cyber-Strafverfolgung und Cyber-Defense brauche. Erneut wurde zudem über die Beziehungen zur EU diskutiert. Die Regierung präsentierte die umstrittene Schiedsgerichtslösung zur Streitbeilegung und bekräftigte ihren Willen, die flankierenden Massnahmen zur Personenfreizügigkeit aufrecht erhalten zu wollen. Der Bundesrat informierte zudem über den Stand der Agrarpolitik 2022 (AP22+). Der dafür verantwortliche Bundesrat, Johann Schneider-Ammann war nicht anwesend, weil er auf einer Reise in die Mercosur-Staaten war.
Ende August fanden die Gespräche – wie einmal pro Jahr üblich – in Form einer Klausur statt. Der Bundesrat trat in corpore an und die einzelnen Magistratinnen und Magistraten stellten die Schwerpunkte ihrer Departemente und die Jahresziele 2019 vor. Auch in Klausur waren die Verhandlungen über ein institutionelles Abkommen mit der EU wichtiges Diskussionsthema.
Dies galt auch für die Gespräche vom 9. November. Erneut war deshalb neben Bundespräsident Alain Berset und Bundeskanzler Walter Thurnherr auch Aussenminister Ignazio Cassis anwesend, begleitet von Johann Schneider-Ammann, der über die Herausforderungen der Aussenhandelspolitik etwa auch aufgrund der Neuorientierung der Handelspolitik der USA berichtete. Beim Rahmenabkommen betonten alle Parteien, dass die roten Linien eingehalten werden müssten. Auch der

Migrationspakt war Gegenstand der Gespräche.

Ende September 2018 hatte Nationalrätin Sibel Arslan (basta, BS) eine Interpellation eingereicht (Ip. 18.3953), mit der sie anfragte, weshalb die Nicht-Regierungsparteien (GP, GLP, BDP), die immerhin rund 16 Prozent der Wählerinnen und Wähler vertreten, nicht zu den Gespräche eingeladen werden. Der Bundesrat schaffe hier eine Zweiklassengesellschaft und überdies hätten die Gespräche keine rechtliche Grundlage. In seiner Antwort – kurz nach den letzten von-Wattenwyl-Gesprächen vom 9. November – machte der Bundesrat deutlich, dass für ihn der Austausch mit allen Parteien von Bedeutung sei, dass es aber für die Regierungsparteien und ihre Bundesrätinnen und Bundesräte die Möglichkeit für einen vertieften Dialog geben müsse, um politische Spielräume ausloten zu können. Die nicht an den Gesprächen beteiligten Fraktionen werden nachträglich mit den Unterlagen für die Gespräche bedient. [61]

Organisation der Bundesrechtspflege

BERICHT
DATUM: 20.04.2018
MARC BÜHLMANN

Internationaler Terrorismus, organisierte Kriminalität, Wirtschaftskriminalität und Cyber-Crime würden nach neuen Strategien und Arbeitsmethoden für die Bundesanwaltschaft rufen, denen aber gleichzeitig von der nationalen Strafrechts- und Prozessgesetzgebung enge Grenzen gesetzt würden, hielt der **Jahresbericht 2017 der Aufsichtsbehörde über die Bundesanwaltschaft** (AB-BA) einleitend fest. Erschwerend komme hinzu, dass die Behörde ihre Verfahren in einem stark politisierten Umfeld führe und deshalb im Fokus der Öffentlichkeit stehe. Die AB-BA habe sich im Berichtsjahr vor allem auf systemische Probleme konzentriert. Unter anderem empfahl sie einen Code of Conduct für ehemalige Mitarbeitende. Positiv beurteilte die Aufsichtsbehörde, dass die operativen Abläufe gut funktionierten und die Mitarbeitenden motiviert seien und Eigeninitiative zeigten. Die AB-BA ging im Bericht zudem ausführlich auf den Fall «Daniel M.» ein, der von der GPDel untersucht wurde. Weiter sei gegen Bundesanwalt Michael Lauber 2017 eine Disziplinarbeschwerde eingereicht worden, auf welche die AB-BA laut Jahresbericht aber nicht eingetreten war. [62]

Aussenpolitik

Beziehungen zu internationalen Organisationen

MOTION
DATUM: 20.09.2011
ANITA KÄPPELI

Die eidgenössischen Räte überwiesen im Berichtsjahr eine Motion Amherd (cvp, VS), welche den Bundesrat aufforderte, auf UNO-Ebene einen Resolutionsentwurf zur Verpflichtung der Staaten einzubringen, Massnahmen zum Schutz der **Kinder vor Missbrauch im Internet** zu ergreifen. Sowohl der Bundesrat als auch die ständerätliche Rechtskommission beantragten die Annahme der Motion. Dieser Empfehlung folgten beide Räte. [63]

INTERNATIONALE BEZIEHUNGEN
DATUM: 16.04.2015
CAROLINE HULLIGER

Le 16 avril, Didier Burkhalter a participé à la **conférence mondiale sur le cyberespace** à La Haye. Il a souligné, dans son discours, que la Suisse était en faveur d'un cyberespace libre, ouvert et sûr, dans lequel s'applique le droit international en vigueur. Rappelons qu'en 2012, le Conseil fédéral avait approuvé la « Stratégie nationale de protection de la Suisse contre les cyberrisques ». [64]

Landesverteidigung

Landesverteidigung und Gesellschaft

POSTULAT
DATUM: 08.06.2010
SÉBASTIEN SCHNYDER

Au mois de juin, le Conseil des Etats a accepté un postulat Recordon (pe, VD) invitant le Conseil fédéral à élaborer un rapport sur les capacités helvétiques à faire face à une **attaque cybernétique** dans ses conséquences civiles et militaires. Le conseiller aux Etats souligne que ces attaques peuvent bloquer totalement ou partiellement les infrastructures et réseaux vitaux d'un pays et paralyser l'armée. [65]

MOTION
DATUM: 15.03.2011
MAXIMILIAN SCHUBIGER

Anfang Juni 2010 hatte der Ständerat ein Postulat Recordon (gp, VD) (Po. 10.3136) überwiesen, welches den Bundesrat beauftragt einen Bericht zu erarbeiten, wie er dem Cyberwar zu begegnen gedenke. Ende Juni desselben Jahres wurde von der SiK-NR unter dem Titel **Massnahmen gegen Cyberwar** eine Motion mit ähnlichem Inhalt eingereicht. Diese beauftragt den Bundesrat mit der Erarbeitung gesetzlicher Grundlagen für Massnahmen zur Sicherung und Verteidigung von Datennetzwerken, die für die Schweiz und für schweizerische Einrichtungen von Bedeutung sind. Vom Nationalrat wurde die Motion in der Wintersession 2010 überwiesen. Nachdem auch der Bundesrat Anfang 2011 die Annahme der Motion beantragte, folgte der Ständerat mit dem gleichen Votum im März 2011. [66]

STUDIEN / STATISTIKEN
DATUM: 01.01.2014
MAXIMILIAN SCHUBIGER

Auch Anfang 2014 publizierte die ETH Zürich ihre gemeinsam mit dem Center for Security Studies (CSS) jährlich erstellte **Jahresstudie „Sicherheit"** zur Ermittlung der Meinungen in den Bereichen Aussen-, Sicherheits- und Verteidigungspolitik in der Schweiz. Augenfällig ist laut der Autoren eine markant positivere Einstellung der Schweizerinnen und Schweizer gegenüber der Armee. 80% der Befragten bejahen die Notwendigkeit der Armee, was einen Anstieg von 8 Prozentpunkten gegenüber 2013 bedeutet. Leicht verlagert hat sich hingegen die Einschätzung der Wehrpflicht. Gegenüber dem Vorjahr sprechen sich 37% für eine Abschaffung der Wehrpflicht zugunsten einer Freiwilligenarmee aus (+ 4 Prozentpunkte), 61% sind dagegen (eine Abnahme um 4 Prozentpunkte). Das Niveau von 2012 (48%) blieb jedoch noch immer weit unterschritten. Auch im Nachgang an die Wehrpflichtabstimmung blieb diese Haltung also gefestigt. Das bevorzugte Wehrmodell bleibt die Milizarmee, welche von einer Mehrheit von 61% (+ 5 Prozentpunkte) unterstützt wird. Einer Abschaffung der Armee stimmten im Berichtsjahr bloss noch 11% der Befragten zu (- 6 Prozentpunkte). Hinsichtlich der anstehenden Weiterentwicklung der Armee (WEA) ist interessant, wie sich die Befragten zu den Armeeausgaben äussern: 2014 hielten 49% die Kosten für angemessen, was einen Anstieg von 5 Prozentpunkten und einen Höchststand seit 1986 bedeutet. Bei der Frage nach Bedrohungsformen stehen Cyber-Angriffe an der Spitze. Auf einer Skala von 1 bis 10 wurde die Eintretenswahrscheinlichkeit eines solchen Ereignisses durchschnittlich auf 5.4 geschätzt. Einen militärischen Angriff fürchten nur gerade 3% der Befragten. Damit einhergehend sehen Schweizerinnen und Schweizer die Funktion der Armee zunehmend in subsidiären Unterstützungs- und Sicherungseinsätzen, wie der Katastrophenhilfe im Inland oder der Unterstützung der zivilen Grenzwache und der Polizei. Auf einer Zehnerskala erreicht die Armee punkto Zufriedenheit mit ihren Leistungen eine Note von 6.3. Gemessen an der langjährigen Entwicklung erreicht zudem die Beurteilung der Verteidigungsausgaben einen Höchstwert: 49% sind 2014 der Auffassung, die Höhe der Ausgaben sei angemessen. Dieser Anstieg um 5% Prozentpunkte entspricht der Abnahme der letztjährigen Einschätzung, die Ausgaben seien zu hoch. Verglichen mit dem Vorjahr, zieht sich die insgesamt positivere Einstellung der Bevölkerung gegenüber der Armee durch alle Befragungsfelder der Studie. [67]

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. [68]

MOTION
DATUM: 13.12.2017
MAXIMILIAN SCHUBIGER

Nationalrat Béglé (cvp, VD) sorgte sich um die **digitale Infrastruktur der Armee**, weswegen er im Herbst 2017 eine Motion dazu formuliert hatte. Konkret stellte der Christlichdemokrat auch einen Zusammenhang zu den neu zu beschaffenden Kampfflugzeugen her, weil gerade diese weitestgehend über Bordcomputer funktionieren und gesteuert werden. Der Motionär sah eine Gefahr darin, dass viele Bestandteile, die die Armee verwendet, von ausländischen Herstellern stammten und es nicht auszuschliessen sei, dass in elektronischen Steuerelementen auch versteckte Funktionen eingebaut würden, die unter Umständen aktiviert werden könnten, um die Systeme fernzusteuern oder zu stören. Gerade bei Fliegern sei das eine grosse Gefahr. Zwar sei das zu Friedenszeiten nicht wahrscheinlich, so der Motionär, falls es aber in den Herstellerstaaten zu einer Destabilisation kommen würde, könnten solche Szenarien eintreffen. Es sei deswegen notwendig, gerade bei der Beschaffung neuer Kampfjets ein zusätzliches Kriterium hinzuzufügen. Neben der geforderten Leistung und dem Preis der Jets sollte auch die „digitale Unabhängigkeit" ausschlaggebendes Kriterium sein. Zusätzlich sollte mit der Motion der Bundesrat aufgefordert werden, für zahlreiche andere Systeme Massnahmen zu ergreifen, um sie vor Cyberangriffen zu schützen.
Der Bundesrat zeigte sich in seiner Stellungnahme einsichtig und äusserte das Bewusstsein der Regierung um diese Gefahren und Entwicklungen. Entsprechend habe sie bereits Schritte unternommen, um diesen Cyberrisiken zu begegnen. Es wurde auch auf den Bericht der Expertengruppe über die Luftverteidigung der Zukunft verwiesen, wo man sich namentlich um Aspekte der Risiken bezüglich der computergestützten Software in Kampfjets gewidmet hatte. Der Bundesrat zeigte sich zwar einsichtig bezüglich der Notwendigkeit, die digitalen Infrastrukturen zu schützen, er beantragte dem Parlament jedoch, die Motion abzulehnen. Die Regierung stellte sich auf den Standpunkt, dass es unmöglich sei, gewollte oder ungewollte Schwachstellen in computergestützten Systemen ausfindig zu machen sowie dass es zahlreiche koordinierte Massnahmen brauche, um derartige Risiken im Cyberbereich zu minimieren. Vor dem Hintergrund anderer in die Wege geleiteter Massnahmen im Cyberbereich wollte man jedoch weitere Ergebnisse abwarten. Die Motion Béglé solle dem nicht vorgreifen.

Im Nationalrat gab es kaum eine Debatte zum Geschäft, es äusserten sich lediglich der Motionär und der Verteidigungsminister. Ersterer warb dabei erfolgreich für sein Anliegen, so dass ihm die Nationalrätinnen und Nationalräte folgten und mit 91 zu 76 Stimmen die Motion annahmen. Acht enthielten sich. [69]

MOTION
DATUM: 31.05.2018
MAXIMILIAN SCHUBIGER

Die **digitale Infrastruktur der Armee** wurde in der Sommersession 2018 mit der Motion von Claude Béglé (cvp, VD) im Ständerat zum Thema. Zwar hatte der Nationalrat zuvor den Vorstoss angenommen, die SiK des Ständerates wollte jedoch die Ablehnung der Motion durchsetzen. Eine Sistierung der Motion, um bereits in Angriff genommene Massnahmen abzuwarten, namentlich die Erarbeitung der Nationalen Strategie zum Schutz vor Cyberrisiken (NCS) und des Aktionsplans Cyberdefence (APCD), wurde diskutiert, jedoch abgelehnt. In der Kommission war man sich einig, dass im Lichte der fortgeschrittenen Digitalisierung relevante Punkte durch den Motionär angesprochen worden sind, der Vorstoss sei insgesamt jedoch zu umfangreich formuliert und ziehe womöglich nicht abschätzbare und hohe Kosten nach sich. Oben erwähnte Massnahmen würden zudem bereits zu weiten Teilen die neuen Herausforderungen durch die Digitalisierung angehen. Dies sei bereits eine adäquate Reaktion des Bundes und es sei deswegen davon abzusehen, die Motion anzunehmen.
Das Ratsplenum sah das offenbar gleich, die Motion wurde nach einer umfangreichen Berichterstattung durch Kommissionssprecher Français (fdp, VD) abgelehnt. [70]

Militärorganisation

POSTULAT
DATUM: 16.06.2017
MAXIMILIAN SCHUBIGER

Armee 2.0 – unter dieses Schlagwort setzte Postulant Dobler (fdp, SG) die Forderungen aus seinem Vorstoss. Die Schweiz müsse das **Technologie-Know-how fördern und sichern** und entsprechend auch im Bereich der Landesverteidigung Modifikationen vornehmen, erklärte er. Fünf Punkte wurden vom St. Galler umschrieben: Das Armeepersonal müsse in Anbetracht des technologischen und wissenschaftlichen Kompetenzbedarfs rekrutiert werden; der Personalbedarf im Bereich Cyberabwehr müsse abgeklärt werden; der Bundesrat solle prüfen, inwiefern mit Bildungsinstitutionen und der Wirtschaft zusammengearbeitet werden könne; Armeeangehörigen sollten diverse neue Typen von Ausbildungen und Einsätzen angerechnet werden können; sowie, fünftens, sollten neue Kriterien der Diensttauglichkeit formuliert werden („differenzierte Tauglichkeit"). Dobler reihte sich damit in eine Gruppe von Parlamentariern ein, welche die Armee bezüglich neuerer Bedrohungsszenarien aus dem Cyberspace und durch computergestützte Systeme besser aufstellen möchte. Technologie und Wissenschaft seien immer wichtiger für die Armee und solch hoch innovativer Themen müsse sich das Militär zuwenden, so der Postulant in seiner Begründung. Einzelne Möglichkeiten zur Anrechenbarkeit von Praktika bei Bundesbetrieben oder Hochschulen an die Dienstleistung seien zwar bereits gegeben, man müsse aber noch weitere Anreize schaffen. Im Fokus stünden dabei Projekte, die für das Militär einen Verwendungszweck haben. Der Bundesrat teilte offensichtlich die Stossrichtung des Postulats und beantragte dessen Annahme. Als es im Sommer 2017 im Nationalrat behandelt wurde, gab es keine Debatte, das Geschäft wurde diskussionslos angenommen. [71]

ANDERES
DATUM: 09.11.2017
MAXIMILIAN SCHUBIGER

Seit einigen Jahren arbeitet der Bund, gemeinsam mit mehreren weiteren Akteuren, an verschiedenen Programmen zur Bewältigung neuer Bedrohungen aus dem digitalen Raum. Diesen als „Cyber-Risiken" umschriebenen, im Zuge der Digitalisierung vermehrt auftretenden Komplikationen und/oder Angriffen wird unter anderem auch mit einer Cyber-Strategie begegnet. Diese Strategie wird dezentral umgesetzt, wobei die Melde- und Analysestelle Informationssicherung (MELANI) eine zentrale Rolle innehat. Damit ist aufgrund des Kooperationsmodells bei MELANI zwischen ISB und NDB direkt auch der Nachrichtendienst des Bundes involviert. Innerhalb des VBS hat aber auch die Armee den Auftrag, sensible IT-Infrastrukturen und Systeme zu schützen. Dafür wurde bis anhin auf die Nutzung sicherer Netze vertraut, gerade auch im militärischen Tagesbetrieb. Zur Informations- und Objektsicherheit wurde zudem innerhalb des Verteidigungsdepartementes eine gleichnamige Stelle eingerichtet. Um nun der weiteren Entwicklung im Cyberbereich zu begegnen, wurde ein **Aktionsplan Cyber-Defence** ausgearbeitet. Diese auf Anregung von Departementsvorsteher Guy Parmelin 2016 lancierte Massnahme soll bis 2020 umgesetzt werden und die bereits laufenden Vorgänge im Rahmen der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken ergänzen.

Der Aktionsplan Cyber-Defence ist ein rein auf das VBS bezogenes Strategiepapier, das mit einer Standortbestimmung im Sommer 2016 angestossen worden war und im folgenden Herbst eine Strategie hervorgebracht hatte, deren Umsetzungsplan im Sommer 2017 verabschiedet wurde. Gemäss dem Aktionsplan ist dieser vorerst als Orientierungshilfe anzusehen, er bedeute jedoch einen zwingenden ersten Schritt, weil eine Anpassung an neue „Herausforderungen im Cyber-Raum ein wichtiges Thema unserer Sicherheitspolitik geworden ist."
Als operative Ziele wurden drei Bereiche definiert. Das VBS soll erstens seine eigenen Systeme und Infrastrukturen jederzeit schützen und verteidigen können. Zweitens soll es möglich werden, militärische und nachrichtendienstliche Operationen im Cyber-Raum durchzuführen. Ferner sollen drittens zivile Behörden im Falle von Cyber-Angriffen unterstützt werden können. Diese Zielvorgaben verlangen jedoch eine genügende Ausstattung mit finanziellen, aber auch personellen Ressourcen – ein Unterfangen, das auf der politischen Bühne auszutragen sein wird.

Die Rekrutierung von geeignetem Milizpersonal beispielsweise mittels neu zu schaffender Cyber-RS, wie im Parlament inzwischen gefordert wurde, wurde im Aktionsplan als nicht zielführend beschrieben. Im Papier ist von einem Bedarf von 166 Stellen die Rede, wovon etwa 100 neu zu schaffen wären. Bezüglich Finanzierung wurden keine präzisen Zahlen genannt, eine Schätzung geht jedoch von etwa 2 Prozent des Jahresbudgets des VBS aus. Ob der gesamte Bereich der Cyber-Abwehr, also auch ausserhalb des VBS und der Armee, durch ein Cybersecurity-Kompetenzzentrum organisiert werden könnte, wurde im Aktionsplan nicht genauer ausgeführt. Unter der

Bezeichnung „CYD-Campus" wurde jedoch eine Plattform zur vertieften Zusammenarbeit skizziert, deren Entwicklung noch abgewartet werden muss. [72]

Bevölkerungsschutz

ANDERES
DATUM: 20.03.2014
MAXIMILIAN SCHUBIGER

Am 20. März 2014 fand die **zweite Cyber-Landsgemeinde** des Sicherheitsverbundes Schweiz (SVS) in Bern statt. Ziel dieses Treffens von rund 70 Vertretern von Bund und Kantonen war es, über den aktuellen Stand der Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) zu informieren. Seit Ende 2013 befassen sich vier paritätisch zusammengesetzte Arbeitsgruppen mit der Umsetzung einzelner Massnahmen der Strategie in den Kantonen. Ziel dieser Massnahmen ist es, mittels konkreter Produkte die Kantone zu unterstützen, ihre Widerstandsfähigkeit zu erhöhen und Cyber-Risiken zu reduzieren. Drei Arbeitsgruppen erarbeiten in den Bereichen Risikoanalyse und Präventionsmassnahmen, Incident Management und Krisenmanagement Konzepte, Prozesse und fördern den Zugang zu Expertenwissen. Die vierte Arbeitsgruppe dokumentiert Straffälle und erstellt ein Konzept zur Koordination von interkantonalen Fallkomplexen. Der Sicherheitsverbund Schweiz koordiniert in Zusammenarbeit mit der Koordinationsstelle NCS, die beim Informatiksteuerungsorgan des Bundes angesiedelt ist, die Umsetzung der Strategie auf Stufe der Kantone und der Gemeinden. [73]

ANDERES
DATUM: 30.04.2014
MAXIMILIAN SCHUBIGER

Per Ende April 2014 lag der **Jahresbericht 2013 des Steuerungsausschusses der nationalen Strategie zum Schutz vor Cyber-Risiken** (NCS) vor. Bei vielen der 16 gefassten Massnahmen, vor allem in den Bereichen Prävention und Reaktion, wurden Ende 2013 bereits erste Meilensteine erreicht. So wurden die notwendigen Schritte zur Erstellung eines Lagebildes, das über die Cyber-Bedrohungen Auskunft geben wird, eingeleitet. In den beteiligten Verwaltungseinheiten beim Bund wurden auch nötige, neue Organisationsstrukturen geschaffen, um Cyber-Bedrohungen rasch erkennen zu können und die Handlungsfähigkeit zu erhöhen. Es wurden Grundlagen für die Zusammenarbeit geschaffen sowie einheitliche Methoden unter den beteiligten Stellen etabliert, damit im Falle von Cyber-Angriffen optimal reagiert und Schäden und Auswirkungen möglichst gering gehalten werden können.
Im Rahmen der Mitte 2012 gestarteten NCS verfolgt der Bundesrat drei strategische Ziele: die frühzeitige Erkennung der Bedrohungen und Gefahren im Cyber-Bereich, die Erhöhung der Widerstandsfähigkeit von kritischen Infrastrukturen sowie eine wirksame Reduktion von Cyber-Risiken. Die Koordination der Umsetzungsarbeiten übernahm die bei der Melde- und Analysestelle Informationssicherung (MELANI) angesiedelte Koordinationsstelle NCS. Dort werden die Umsetzungsarbeiten überwacht und für den Einbezug aller Beteiligten gesorgt. Zusammen mit den verantwortlichen Bundesämtern wurden die Meilensteine und der Zeitplan für die jeweiligen Massnahmen definiert und in einer Roadmap festgehalten. [74]

Infrastruktur und Lebensraum

Verkehr und Kommunikation

Post und Telekommunikation

MOTION
DATUM: 20.09.2011
SUZANNE SCHÄR

Die Räte überwiesen eine Motion Barthassat (cvp, GE), die eine **Verlängerung der Aufbewahrungspflicht für Protokolle über die Zuteilung von IP-Adressen** verlangte. Der Bundesrat unterstützte den Vorstoss mit dem Hinweis, dass eine entsprechende Anpassung des Bundesgesetzes vom 6. Oktober 2000 betreffend Überwachung des Post- und Fernmeldeverkehrs im Rahmen der laufenden Totalrevision vorgesehen sei. Zum strafrechtlichen Aspekt (Cyberkriminalität) siehe hier. Zum Schutz der Kinder vor Pornografie siehe auch hier. [75]

POSTULAT
DATUM: 23.12.2011
SUZANNE SCHÄR

In der Frühlings- und in der Dezembersession nahm der Nationalrat stillschweigend zwei Postulate an, die den Schutz der digitalen Infrastruktur einerseits und den Schutz ihrer Nutzer andererseits forderten. Ein Postulat Darbellay (cvp, VS) wünschte – unter Einbezug aller Sicherheitskräfte, einschliesslich der Armee – die Erarbeitung eines Konzepts zum Schutz der digitalen Infrastrukturen der Schweiz. Das Postulat Schmid-Federer (cvp, ZH) (11.3906) verlangte vom Bundesrat die **Prüfung eines umfassenden Grundlagengesetzes für die Datenverkehrsnetze** (IKT-Grundlagengesetz). [76]

Bildung, Kultur und Medien

Medien

Medienpolitische Grundfragen

MOTION
DATUM: 16.03.2011
DEBORA SCHERRER

Der Gesetzgeber beschäftigte sich im Berichtsjahr vornehmlich mit der SRG und der Teilrevision zum Radio- und Fernsehgesetz. Die Motion für ein „**Neues System für die Erhebung der Radio- und Fernsehgebühren**" wurde vom Ständerat überwiesen, nachdem der Nationalrat sie bereits 2010 angenommen hatte. Ein Postulat und eine Motion Fehr (sp, SH), die einen Bericht und ein Observatorium zu den Dynamiken im Internet forderten, um damit auch den gezielten Umgang mit neuen Medien zu fördern, wurden in der grossen Kammer hingegen abgelehnt. Weiter setzte der Bundesrat auf die Selbstregulierung der Medien. [77]

Neue Medien

INTERNATIONALE BEZIEHUNGEN
DATUM: 29.03.2000
ELISABETH EHRENSPERGER

Aufgrund der Internationalität und Anonymität des weltweiten Datennetzes stellen illegale Inhalte insbesondere rassistischer und pornographischer Art oder die Abwicklung krimineller Handlungen über das Internet die Bundesbehörden vor zahlreiche ungelöste Probleme. Klar schien zu sein, dass diese nicht alleine, sondern nur im Rahmen einer **internationalen Kooperation** zu lösen seien. Im Rahmen einer Holocaust-Gedenkkonferenz in Stockholm rief Bundesrätin Dreifuss zum Kampf gegen den Rassismus im Internet auf. Mit ihrer Forderung nach internationaler Kooperation und neuen rechtlichen Instrumenten griff Dreifuss ein kontroverses Thema auf. Insbesondere die USA, Grossbritannien und Schweden zeigten sich hinsichtlich Eingriffen in das Internet und andere Medien skeptisch aufgrund ihrer Ablehnung jeglicher Einschränkung der **Meinungsäusserungsfreiheit**. Dem Bundesamt für Auswärtige Angelegenheiten (EDA) war es dennoch gelungen die Thematik auf die Traktandenliste der 2001 in Afrika stattfindenden Weltkonferenz gegen Rassismus, Rassendiskriminierung, Fremdenhass und Intoleranz zu setzen. Anlässlich eines Vorbereitungsseminars zu dieser Konferenz wurde im Februar ein provokatives Arbeitspapier des Basler Rechtsprofessors **David Rosenthal** diskutiert, in welchem dieser betonte, die Ahndung illegaler Inhalte im Internet scheitere entgegen gängiger Meinung nicht an juristischen oder technischen Problemen als vielmehr am fehlenden politischen Willen. [78]

ANDERES
DATUM: 05.06.2000
ELISABETH EHRENSPERGER

Im Mai hatte der Virus „**I love you**" einen grossen Teil der Kommunikation in der Bundesverwaltung für einen Tag lahmgelegt; zwischen 400 und 500 Personalcomputer waren laut Bundesamt für Informatik infiziert und deren Festplatten vollständig gelöscht worden. Der Virusangriff habe die Verwaltung damit rund eine Mio Fr. gekostet. Über mögliche durch „I love you" in der Privatwirtschaft verursachte Schäden hielt sich diese aus Imagegründen – um nicht heikle Lücken in ihrem Sicherheitsdispositiv preisgeben zu müssen – bedeckt. [79]

ANDERES
DATUM: 24.10.2000
ELISABETH EHRENSPERGER

Im Versuch, gegen **illegale Inhalte im Internet** anzukämpfen, verabschiedete die Bundespolizei (Bupo) im April Verhaltensgrundsätze, die abgestützt auf ein Rechtsgutachten des Bundesamts für Justiz den Providern als private Anbieter elektronischer Dienstleistungen eine aktive Rolle beim Kampf gegen illegale Websites-Inhalte zuteilten. So sollten Provider, die den Nutzerinnen und Nutzern den Zugang zum Internet verschaffen, bei Erhalt eines Hinweises der Strafverfolgungsbehörden illegale Netzinhalte sperren. Das Gutachten baute auf einem Bundesgerichtsentscheid von 1999 auf, das einen Buchhändler mit der Begründung verurteilt hatte, bei Rassendiskriminierung und harter Pornographie seien nicht nur der Autor, sondern

auch weitere Verbreiter strafbar. Das Positionspapier der Bupo drohte, eine einvernehmliche Lösung mit den Providern zu verhindern. Da nach wie vor zahlreiche rechtliche Fragen offen standen, liess der Verband Inside Telecom (VIT), Vertreter der Provider, ein Zweitgutachten erstellen. Die Professoren Marcel Niggli, Franz Riklin und Günter Stratenwerth orteten eine eklatante Rechtsunsicherheit, welche die Dringlichkeit gesetzlicher Regelungen spiegelten. Der Unmut der Provider über das Bupo-Papier gründete insbesondere in den Befürchtungen, einerseits eine eigene Überwachungspolizei aufbauen zu müssen und andererseits durch allzu strenge nationale Gesetze einen Standortnachteil im internationalen Umfeld zu erleiden. [80]

POSTULAT
DATUM: 15.12.2000
ELISABETH EHRENSPERGER

Der Nationalrat überwies ein Postulat Ehrler (cvp, AG), das den Bundesrat dazu einlud, gegebenenfalls mit der privaten Wirtschaft zusammen einen aktiven Beitrag für die **Systemsicherheit im Internet** zu leisten. Dabei müssten die Sensibilisierung für Sicherheitsfragen, die Entwicklung von Sicherheitsstandards sowie das Vorbeugen gegenüber kriminellen Machenschaften von Hackern im Mittelpunkt stehen. Zur **Bekämpfung der Internet-Kriminalität** forderte die Zentralschweizer Polizeidirektorenkonferenz eine Koordination auf Bundesebene. Insbesondere in den Bereichen Kinderpornographie sowie Rechtsextremismus und Rassismus seien Abklärungen in den einzelnen Kantonen kaum sinnvoll und ohne zusätzliches Personal bei den kantonalen Polizeikorps überhaupt nicht machbar. [81]

VERWALTUNGSAKT
DATUM: 21.02.2002
ROMAIN CLIVAZ

La multitude de délits pouvant être commis au moyen de l'Internet a poussé le Conseil fédéral à mettre sur pied un Service national de coordination de la **lutte contre la criminalité sur Internet** (SCOCI). C'est suite aux pressions exercées par diverses organisations, notamment de lutte contre la pédophilie, et par les cantons, que le Conseil fédéral a annoncé la création, dès janvier 2003, de cet organe de coordination. Muni d'un budget de 1,3 millions de francs, dont deux tiers à la charge des cantons, et employant 9 personnes, il sera le point de contact central pour les personnes souhaitant signaler l'existence de sites suspects. Il effectuera également des recherches des contenus illicites sur Internet et procèdera à des analyses approfondies dans le domaine de la criminalité sur Internet. (Pour la lutte contre la pédophilie sur Internet, voir aussi ici) [82]

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. [83]

MOTION
DATUM: 20.12.2006
ANDREA MOSIMANN

Der Ständerat überwies in der Sommersession die Motion Schweiger (fdp, ZG), welche Massnahmen zur **Bekämpfung der Cyberkriminalität** und zum Schutz der Kinder auf elektronischen Netzwerken fordert. In der Wintersession wurde im Nationalrat überdies die Motion Hochreutener (cvp, BE; 06.3554) gutgeheissen, die den Bundesrat auffordert, die Massnahmen gegen Internetpornographie, die er aufgrund der Motion Schweiger treffen wird, auch für Gewaltdarstellungen vorzusehen. [84]

MOTION
DATUM: 11.12.2007
ANDREA MOSIMANN

Kinder sollen künftig besser vor harter Pornografie im Internet geschützt werden. Der Nationalrat nahm die Motion Schweiger (fdp, ZG; Mo. 06.3170) zur **Bekämpfung der Cyberkriminalität zum Schutz der Kinder** auf den elektronischen Netzwerken an. Dabei folgte er dem Antrag des Bundesrates, für einen Teil der Massnahmenvorschläge lediglich einen Prüfungsauftrag zu erteilen. Der Ständerat stimmte dieser Änderung in der Wintersession zu und hiess auch die Motion Hochreutener (cvp, BE; Mo. 06.3554) gut, welche fordert, die gegen Internetpornographie getroffenen Massnahmen auch für Gewaltdarstellungen vorzusehen. [85]

VERWALTUNGSAKT
DATUM: 29.02.2008
ANDREA MOSIMANN

Der Bundesrat kündigte im Februar an, er werde die Ressourcen für die Überwachung jihadistischer und gewaltextremistischer Internetseiten aufstocken, um wirksamer gegen die **Netzwerkkriminalität** vorgehen zu können. Keinen Handlungsbedarf sah die Regierung auf gesetzlicher Ebene. Sie stellte sich auf den Standpunkt, dass das geltende Strafrecht die Verantwortlichkeit von Providern und Internetdiensten im Zusammenhang mit Internetkriminalität genügend regle und nahm damit Abstand vom Gesetzesentwurf aus dem Jahr 2004. [86]

MOTION
DATUM: 20.03.2008
ANDREA MOSIMANN

In der Frühjahrssession hiess der Nationalrat eine Motion Glanzmann-Hunkeler (cvp, LU) gut, mit welcher der Bundesrat verpflichtet werden soll, unverzüglich das **Ratifikationsverfahren zur Cybercrime-Konvention** des Europarats einzuleiten. Zudem wurde die Frist für eine parlamentarische Initiative Aeppli Wartmann (sp, ZH; Pa.Iv. 02.452) bis zur Frühjahrssession 2010 verlängert. Dieser Vorstoss zielt auf eine Verbesserung der Strafverfolgung im Bereich der Internetkriminalität. [87]

MOTION
DATUM: 02.06.2008
ANDREA MOSIMANN

Der Ständerat überwies im Berichtsjahr ein Postulat Frick (cvp, SZ) (Po. 08.3101). Der Bundesrat wird damit beauftragt, einen Bericht über den Stand und die Zukunft der öffentlichen **Sicherheit der Schweiz im digitalen Zeitalter** vorzulegen. Unter anderem sollen Wirksamkeit und Effizienz der präventiven und repressiven Massnahmen zur Bekämpfung von Internetkriminalität untersucht werden. Gegen den Willen der Regierung hiess der Rat auch eine Motion Burkhalter (fdp, NE) gut. Sie will den Bund dazu verpflichten, gemeinsam mit den Kantonen und der Wirtschaft eine nationale Strategie für die **Bekämpfung der Internetkriminalität** zu entwickeln. [88]

MOTION
DATUM: 03.06.2009
SABINE HOHL

Der Nationalrat stimmte einer Motion Burkhalter (fdp, NE) zu, die vom Bundesrat die Erarbeitung einer nationalen **Strategie zur Bekämpfung der Cyberkriminalität** fordert. Insbesondere sollen Massnahmen gegen Spionage im Internet und gegen Datenmissbrauch entwickelt werden. Im Vorjahr war die Motion bereits im Ständerat angenommen worden. Der Bundesrat hatte die Ablehnung der Motion empfohlen, dies mit der Begründung, dass die Schweiz bereits über eine Strategie gegen Cyberkriminalität verfüge. [89]

MOTION
DATUM: 23.09.2009
SABINE HOHL

Der Ständerat nahm eine vom Nationalrat im Vorjahr überwiesene Motion Glanzmann-Hunkeler (cvp, LU) an, welche den Bundesrat auffordert, das Ratifikationsverfahren zur **Cybercrime-Konvention** des Europarates unverzüglich aufzunehmen. [90]

MOTION
DATUM: 13.04.2010
SUZANNE SCHÄR

Im Bereich des **Jugendmedienschutzes** überwies der Ständerat im März drei Nationalratsmotionen: Er stimmte der Motion Glanzmann-Hunkeler (cvp, LU) zu, welche die Schaffung gesetzlicher Grundlagen für die Registrierungspflicht von Wireless-Prepaid-Karten als Massnahme gegen Kinderpornografie im Internet verlangt. Damit verbunden überwies er ein Postulat der Kommission für Rechtsfragen (Po. 10.3097), die den Bundesrat auffordert, eine umfassende Strategie zur Ermittlung von Internetstraftätern vorzulegen. Im weiteren nahm er die Motionen von Norbert Hochreutener, (cvp, BE) (Mo. 07.3870) und Evi Allemann (sp, BE) (Mo. 09.3422) an, die ein Verkaufsverbot für Killerspiele fordern. [91]

POSTULAT
DATUM: 08.06.2010
SUZANNE SCHÄR

Mit dem Aufgreifen des digitalen Potenzials und der Entwicklung unterschiedlichster Nutzungsformen und Angebote v.a. im Internet ist in den vergangenen Jahren mit der **Missbrauchsgefahr** auch der Regulierungsbedarf gestiegen. So wurden im National- und Ständerat zahlreiche Vorstösse eingereicht oder behandelt, welche den unlauteren Gebrauch des Internets thematisierten, um ihm mit staatsschützerischen Massnahmen bis hin zum Jugendmedienschutz zu begegnen. In der Sommersession überwies der Ständerat ein Postulat von Luc Recordon (Grüne, VD), das den Bundesrat beauftragte, in einem Sonderbericht darzustellen, inwieweit die Schweiz auf einen möglichen Angriff auf zentrale zivile und militärische Einrichtungen im Internet vorbereitet sei. Damit verbunden war die Aufforderung, die entsprechende Gefahrenlage in den Sicherheitsbericht 2010 einfliessen zu lassen. [92]

INTERNATIONALE BEZIEHUNGEN
DATUM: 18.06.2010
SUZANNE SCHÄR

In Beantwortung der Motion Glanzmann-Hunkeler (cvp, LU; Mo. 07.3629), die 2007 die Ratifizierung der bislang einzigen internationalen Übereinkunft über die **Internetkriminalität** gefordert hatte, unterbreitete der Bundesrat im Juni dem Parlament die „Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität" vom November 2001 zur Annahme. [93]

VERWALTUNGSAKT
DATUM: 06.08.2010
SUZANNE SCHÄR

Im Bestreben, die Sicherheit des elektronischen Datentransfers im Geschäfts- und Behördenverkehr zu erhöhen, lancierte das Staatssekretariat für Wirtschaft Seco Anfang Mai das Pilotprojekt **Suisse-ID**. Der elektronische Identitätsnachweis soll Privaten und Unternehmen einen sicheren Datenaustausch über das Internet bis hin zur Abgabe einer rechtsverbindlichen elektronischen Unterschrift ermöglichen. [94]

MOTION
DATUM: 16.09.2010
SUZANNE SCHÄR

Im September nahm der Ständerat eine Motion von Ivo Bischofberger (cvp, AI) an, welche die Schaffung gesetzlicher Grundlagen für ein **koordiniertes Vorgehen gegen Internetkriminalität und im Bereich des Jugendmedienschutzes** unter der Führung des Bundes fordert. Bislang sind diverse Bundes-, aber auch interkantonale und kantonale Stellen und Sondereinrichtungen mit entsprechenden Präventions- und Schutzaufgaben sowie mit der Strafverfolgung betraut. Der Nationalrat wird die Motion 2011 behandeln. Bereits im Sommer hatte Nationalrätin Barbara Schmid-Federer (cvp, ZH) eine parlamentarische Initiative (Pa. Iv. 10.473) mit gleicher Forderung eingereicht, die im Berichtsjahr noch nicht zur Verhandlung ins Plenum gelangt war. [95]

MOTION
DATUM: 16.09.2010
SUZANNE SCHÄR

In der Herbstsession nahm der Ständerat eine weitere Motion zum Thema Jugendmedienschutz an. FDP-Vertreter Rolf Schweiger (ZG) fordert darin die Entwicklung eines **Medienführerscheins** für Jugendliche samt Verankerung eines Programms zur Förderung der Medienkompetenz im Lehrplan 21. Diese Vorlage sowie zwei im Dezember eingereichte Postulate ähnlicher Stossrichtung waren Ende des Jahres im Nationalrat noch hängig. [96]

GERICHTSVERFAHREN
DATUM: 11.11.2010
SUZANNE SCHÄR

Im Zusammenhang mit dem Internet beschäftigten Fragen zur **Meinungsäusserungs- und Medienfreiheit** sowie zur Handhabung von Personendaten die Gerichte diverser Stufen. Im Februar bestätigte das Bundesgericht ein Urteil der Aargauer Justiz, die den Geschäftsführer einer Einzelfirma wegen Begünstigung verurteilte. Über die Internetplattform der Firma waren ehrverletzende Aussagen über einen Lokalpolitiker verbreitet worden. Statt die IP-Adressen der Plattformbenutzer nach „Bundesgesetz betreffend Überwachung des Post- und Fernmeldeverkehrs" ordnungsgemäss zu speichern und aufzubewahren waren diese gelöscht worden. Das Gericht befand, dass der Geschäftsführer dadurch die Strafverfolgung behindert und sich der Begünstigung einer über das Internet begangenen Straftat schuldig gemacht hatte. Im Fall einer Ehrverletzungsklage hielt das Bundesgericht im November in einem Grundsatzurteil fest, dass der Quellenschutz auch für Blogbeiträge gilt, solange diese ein Minimum an Information beinhalten. Provider könnten nicht dazu verpflichtet werden, die Internetadresse einer Quelle bzw. eines Informationslieferanten herauszugeben. Bei Berufung auf das Redaktionsgeheimnis hätten sie sich jedoch anstelle der Quelle einem allfälligen strafrechtlichen Verfahren zu stellen. [97]

VERWALTUNGSAKT
DATUM: 20.11.2010
SUZANNE SCHÄR

Im Juni verabschiedete der Bundesrat das Programm „**Jugendmedienschutz und Medienkompetenz**", das 2011–2015 vom Bundesamt für Sozialversicherungen koordiniert und umgesetzt werden wird. Im Gegensatz zu den Killerspielvorstössen aus dem Parlament setzt dieses v.a. auf Sensibilisierung und Prävention. Weitergehende Regulierungsmassnahmen auf Bundesebene, wie sie v.a. aus den Reihen der CVP verlangt wurden, gedachte der Bundesrat bis Programmabschluss und dem allfälligen Nachweis eines zusätzlichen Regulierungsbedarfs zurückzustellen. Der Ständerat überwies ein Postulat Savary (sp, VD) (Po. 10.3263), welche die Erstellung eines Berichts zur Praxis des illegalen Herunterladens von Musik im Internet fordert. [98]

MOTION
DATUM: 02.12.2010
SUZANNE SCHÄR

Die grosse Kammer nahm im Dezember eine Motion der Sicherheitskommission des Nationalrats an. Darin wird die Vorbereitung von Gesetzesgrundlagen verlangt, welche die **Sicherung wichtiger ziviler und militärischer Daten(-Netzwerke)** erlauben und regeln. Die Veröffentlichung geheimer Protokolle aus dem Irakkrieg und diplomatischer Depeschen der USA im Oktober 2010 durch die Enthüllungsplattform Wikileaks intensivierten gegen Ende Jahr den öffentlichen Diskurs um die Datensicherheit im Internet. Im Dezember gab der Bundesrat die Einsetzung einer Arbeitsgruppe bekannt, die eine Strategie zur Abwehr von Internetangriffen (Cyber-Defense) zu erarbeiten hat. Bis Ende 2011 soll sie zudem die Bündelung der zwölf dezentralen, mit Cyber-Defense beauftragten Verwaltungsstellen prüfen. [99]

MOTION
DATUM: 11.04.2011
DEBORA SCHERRER

Das **Internet** wird nicht mehr als einheitliches Medium, sondern vielmehr als eine technische Plattform angesehen, auf der verschiedenste Anwendungen möglich sind. Von der Individualkommunikation bis hin zur Massenkommunikation betrifft es zunehmend alle Lebensbereiche. Problemstellungen und Fragen im Zusammenhang mit dem Internet können immer weniger umfassend beantwortet werden. Die Einflüsse der Informations- und Kommunikationstechnologien (IKT) gilt es stärker in die verschiedensten Problemstellungen einzubeziehen. So besteht im Rahmen der medienpolitischen Debatten die Frage, wie sich die Medienlandschaft unter dem Einfluss der neuen Möglichkeiten verändert und wo allenfalls politischer Handlungsbedarf besteht.

Der mit der Missbrauchsgefahr des Internets einhergehende Regulierungsbedarf hatte im Berichtsjahr weiterhin einen hohen Stellenwert auf der politischen Agenda. Zwei von Hans-Jürg Fehr (sp, SH) 2009 eingereichte politische Vorstösse, welche die **Überwachung des Internets** thematisierten, wurden im Berichtsjahr vom Nationalrat abgelehnt. In einem Postulat (Po. 09.3628) hatte Fehr vom Bundesrat einen Bericht über Gegenwart und Zukunft des Internets in der Schweiz und in der Folge in einer ebenso gescheiterten Motion ein Internetobservatorium gefordert. Dieses hätte die Entwicklung des Internets in der Schweiz und im Ausland in all seinen Facetten beobachten sollen, um dann dem Bundesrat und den eidgenössischen Räten regelmässig den politischen Handlungsbedarf aufzuzeigen. Der Bundesrat sah aufgrund der bereits lancierten Massnahmen wie etwa der „Strategie für eine Informationsgesellschaft in der Schweiz" keinen zusätzlichen Handlungsbedarf. Zudem wies er darauf hin, dass das Internet kein einheitliches Phänomen sei, das durch einen Bericht oder ein Observatorium genügend thematisiert und überwacht werden könne. [100]

1) AB NR, 1994, S. 1204 f.; AB NR, 1994, S. 614 f.; Presse vom 2.2.94.
2) Medienmitteilung Bundesrat vom 26.04.2017
3) AB SR, 2015, S. 128 f.
4) Medienmitteilung Bundesrat vom 26.04.2017; NCS Bericht Wirksamkeitsueberpruefung
5) AB SR, 2017, S. 661 ff.; LZ, TA, 20.9.17
6) AB SR, 2017, S. 701 ff.; SGT, 26.9.17
7) AB NR, 2017, S. 1994 ff.; Bericht SiK-NR vom 30.10.2017; SGT, TA, TG, 8.12.17
8) AB NR, 2017, S. 2138 f.; Bericht SiK-NR vom 30.10.2017
9) AB NR, 2018, S. 87 f.; NZZ, 3.3.18
10) AB NR, 2018, S. 217 f.
11) AB SR, 2018, S. 110 f.; Bericht SiK-SR vom 30.10.2017; CdT, 7.3.18
12) AB NR, 2018, S. 210 f.
13) Bericht NCS 2018-2022; Medienmitteilung Bundesrat vom 19.04.2018
14) BWL (2018). Minimalstandard zur Verbesserung der IKT-Resilienz; Medienmitteilung BR vom 27.8.18
15) AB SR, 2018, S. 602 ff.; Bericht SiK-SR vom 13.8.18
16) AB NR, 2018, S. 1922; AB SR, 2018, S. 313 f.; Kommissionsbericht RK-NR vom 25.10.2018 (18.3379)
17) AB NR, 2012, S. 703 f.
18) AZ, 11.4.14
19) Medienmitteilung SPK-NR vom 29.8.14
20) AB NR, 2014, S.111 f.

21) AB SR, 2015, S. 734; Kommissionsbericht WBK-SR vom 22. Juni 2015; NZZ, 9.9.15
22) AB NR, 2008, S. 467; AB SR, 2008, S. 365 ff.
23) AB SR, 2010, S. 1020 f. AB NR, 2010, S. 551 (Mo. Darbellay).
24) AB SR, 2011, S. 251 f.
25) AB NR, 2011, S. 531; SoS, 5.11.11
26) AB NR, 2011, S. 531
27) NZZ, 4.10.12; Presse vom 28.9, 1., 5. Und 17.10.12.
28) NZZ, 28.6.12.
29) BBl, 2013, S. 563 ff.; Medienmitteilung IBS vom 15.5.13 .pdf
30) Informatiksicherheit im Nachrichtendienst des Bundes. Bericht der Geschäftsprüfungsdelegation (Zusammenfassung); NZZ, 2.5. und 2.11.13
31) AB NR, 2014, S. 201; AB SR, 2014, S. 415 ff.; NZZ, 2.5.14.
32) Erläuternder Bericht zum Entwurf eines Bundesgesetzes über die Informationssicherheit; Vernehmlassungsbericht Informationssicherheitsgesetz
33) Medienmitteilung BR vom 4.5.17; Medienmitteilung BR vom 5.4.17
34) AB SR, 2017, S. 842 ff.; BBl, 2017, S. 2359 ff.
35) AB NR, 2018, S. 377 ff.
36) Medienmitteilung BR vom 26.4.18
37) AB SR, 2018, S. 767 f.; BaZ, 27.9.18
38) Medienmitteilung SiK-NR vom 9.10.18; NZZ, 10.10.18
39) 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
40) NZZ, 15.1., 3.3. und 1.4.92
41) 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.
42) AB NR, 1994, S. 1250; AB NR, 1994, S. 329 ff.; AB NR, 1994, S. 869 ff.; AB SR, 1994, S. 1074; AB SR, 1994, S. 14 ff.; AB SR, 1994, S. 430 f.; AB SR, 1994, S. 582; AB SR, 1994, S. 775; AB SR, 1994, S. 880; BBl, 1994, III, S. 256 ff.
43) AB NR, 1998, S. 2842 f.; NZZ, 31.7., 8.8. und 14.8.98; AT, 4.8.98; BZ, 5.8.98.
44) AB SR, 2001, S. 27 f.; AB NR, 2001, S. 1087 ff.
45) 24h, 4.4.06. ; Motion Schweiger: AB SR, 2006, S. 397 ff.; Motion Hochreutener: AB NR, 2006, S. 2027.
46) AB NR, 2007, S. 1134 ff.; AB SR, 2007, S. 1060 f.
47) AB NR, 2011, S. 150 ff.
48) AB NR, 2011, S. 150 ff.
49) AB NR, 2011, S. 100 ff.; AB NR, 2011, S. 96 ff.; AB SR, 2011, S. 340
50) Pa.Iv. 10.473
51) AB NR, 2011, S. 528
52) AB NR, 2011, S. 528; AB SR, 2011, S. 855 f.
53) Medienmitteilung VBS vom 20.3.2014.pdf
54) Lit. Fedpol 2014; Medienmitteilungen Fedpol vom 8.5.14.pdf
55) Medienmitteilung NCSC (damals Melani) vom 11.9.14
56) Medienmitteilung ISB vom 20.11.14.pdf
57) AB NR, 2016, S. 1801
58) AB NR, 2017, S. 1685
59) AB SR, 2018, S. 209 f.; Bericht RK-SR vom 12.2.18
60) AB NR, 2018, S. 535; Po. 17.4295
61) Ip. 18.3953; Medienmitteilung BR vom 2.2.18; Medienmitteilung BR vom 31.8.18; Medienmitteilung BR vom 4.5.18; Medienmitteilung BR vom 9.11.18
62) Tätigkeitsbericht 2017 AB-BA
63) AB NR, 2011, S. 529; AB SR, 2011, S. 855.
64) Communiqué du 14.04.2015
65) BO CE, 2010, p. 550.
66) AB NR, 2010, S. 1800 ff., AB SR, 2011, S. 251 f., AB SR, 2010, S. 550.
67) lit. Szvircsev Tresch und Wenger (2014). Sicherheit 2014
68) AB NR, 2015, S. 420 f.; BBl, 2014, S. 8909 ff.
69) AB NR, 2017, S. 2143 f.
70) AB SR, 2018, S. 358 ff.; Bericht SiK-SR vom 19.3.18
71) AB NR, 2017, S. 1196
72) Aktionsplan Cyberdefence
73) Medienmitteilung VBS vom 20.3.14.pdf
74) Jahresbericht Steuerungsausschuss NCS 2013.pdf; Medienmitteilung VBS vom 30.4.14.pdf
75) AB NR, 2011, S. 528; AB SR, 2011, S. 856 f.
76) AB NR, 2011, S. 531, 2266.
77) AB SR, 2011, S. 1360 ff. AB NR, 2011, S. 594.
78) TA, 12.1.00; CdT, 12.2.00; Presse vom 28.1. und 18.2.00; Bund, 29.3.00.68
79) NF, 5.6.00.
80) BZ, 10.5.00; 24h, 16.5.00; Presse vom 16.5. und 24.10.00; NZZ, 19.5.00.
81) AB NR, 2000, S. 1605.; NZZ, 28.11.00.
82) Presse du 21.2.02.
83) NZZ, 11.12.04. Siehe auch Lit. Moreillon.
84) AB SR, 2006, S. 397 (Schweiger); AB NR, 2006, S. 2027 (Hochreutener).
85) AB NR, 2007, S. 1134 ff.; AB SR, 2007; S. 1060.
86) Bund, LT und NF, 29.2.08.
87) AB NR, 2008, S. 467 und 461
88) AB SR, 2008, S. 365 ff.
89) AB NR, 2009, S. 1005.
90) AB SR, 2009, S. 962.
91) AB SR 2010, S. 354 f.; NZZ, 13.4.10.
92) AB SR, 2010, S. 550.
93) BBl, 2010, S. 4697 ff.
94) SGT, 4.5.10; NZZ, 4.5. und 6.8.10.
95) AB SR 2010, S. 825 f.SGT, 5.7.2010; NZZ, 17.9.10.
96) AB SR 2010, S. 823 ff.; NZZ, 17.9.10.
97) BGE 69 IV 118, BaZ, 2.2.10; BGE 136 IV 145; NZZ, 11.11.10.
98) Medienmitteilung EDI, 14.6.10; AB NR 2010, Beilagen Wintersession, S. 370 f.; NZZ, 20.11.10.
99) AB NR, 2010, S. 1800 ff.; NZZ, 3.12. und 11.12.10; CdT, 11.12.10.
100) AB NR, 2011, S. 594; AB NR, 2011, S. 594.