année politique suisse

DOKUMENTATION · ANALYSE · DIFFUSION

Ausgewählte Beiträge zur Schweizer Politik

Suchabfrage	**19.04.2019**
Thema	**Keine Einschränkung**
Schlagworte	**Spionage**
Akteure	**Keine Einschränkung**
Prozesstypen	**Keine Einschränkung**
Datum	**01.01.1990 - 19.04.2019**

Impressum

Herausgeber

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

Beiträge von

Ackermann, Nadja
Bühlmann, Marc
Frick, Karin
Hohl, Sabine

Bevorzugte Zitierweise

Ackermann, Nadja; Bühlmann, Marc; Frick, Karin; Hohl, Sabine 2019. ***Ausgewählte Beiträge zur Schweizer Politik: Spionage, 2009 - 2018***. Bern: Année Politique Suisse, Institut für Politikwissenschaft, Universität Bern. www.anneepolitique.swiss, abgerufen am 19.04.2019.

Inhaltsverzeichnis

Abkürzungsverzeichnis

VBS	Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport
AHV	Alters- und Hinterlassenenversicherung
SiK-SR	Sicherheitspolitische Kommission des Ständerates
GPK	Die Geschäftsprüfungskommissionen
SiK-NR	Sicherheitspolitische Kommission des Nationalrates
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
GPDel	Geschäftsprüfungsdelegation
RK MZF	Regierungskonferenz Militär, Zivilschutz und Feuerwehr
KMU	Kleine und mittlere Unternehmen
BWIS	Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit
fedpol	Bundesamt für Polizei
SGV	Schweizerischer Gewerbeverband
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NDB	Nachrichtendienst des Bundes (bis 2010: Strategischer Nachrichtendienst und Dienst für Analyse und Prävention)

DDPS	Département fédéral de la défense, de la protection de la population et des sports
AVS	Assurance-vieillesse et survivants
CPS-CE	Commission de la politique de sécurité du Conseil des Etats
CdG	Les Commissions de gestion
CPS-CN	Commission de la politique de sécurité du Conseil national
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
PME	petites et moyennes entreprises
LMSI	Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure
fedpol	Office fédéral de la police
USAM	Union suisse des arts et métiers
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
SRC	Service de renseignement de la Confédération (à 2010: Service de renseignement stratégique et Service d'analyse et de prévention)

Allgemeine Chronik

Grundlagen der Staatsordnung

Rechtsordnung

Innere Sicherheit

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. [1]

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. [2]

BERICHT
DATUM: 05.05.2014
NADJA ACKERMANN

Im Mai 2014 kommunizierte der Nachrichtendienst des Bundes (NDB) in seinem **Lagebericht zur Sicherheit des NDB 2014** seine aktuellen Einschätzungen der Sicherheitsgefährdungen in der Schweiz. Dabei hob er die vergleichsweise stabile und ruhige sicherheitspolitische Situation hervor. Die Schweiz sei weiterhin kein prioritäres Ziel dschihadistisch motivierter Anschläge. Im Brennpunkt des Lageradars lägen die Wirtschaftsspionage und die Spionage gegen sicherheitspolitische Interessen der Schweiz. [3]

ANDERES
DATUM: 13.06.2014
NADJA ACKERMANN

Im Juni warf die **Affäre um Dominique Giroud** hohe Wellen. Der Walliser Weinhändler, gegen den in der Waadt Strafverfahren wegen Betrugs, Waren- sowie Urkundenfälschung liefen und in Genf wegen Steuerbetrugs ermittelt wurde, hatte versucht, zwei Westschweizer Journalisten auszuspionieren. Diese hatten zuvor brisante Informationen über Giroud veröffentlicht. Kurz darauf kam aus, dass der von Giroud angeheuerte Privatdetektiv selbst dem Westschweizer Fernsehen heikle Informationen über den Weinhändler zugespielt hatte.
Da am Spionageversuch nicht nur ein Privatdetektiv und ein Hacker, sondern auch ein Mitarbeiter des schweizerischen Nachrichtendiensts (NDB) beteiligt war, schwappte der Fall bis nach Bundesbern. Hier hatte sich die Geschäftsprüfungsdelegation (GPDel) als Aufsichtsbehörde des NDB mit der Frage zu befassen, ob das Risikomanagement des Nachrichtendiensts funktioniert hatte. Der Fall offenbarte dabei Mängel bei der Auswahl und Führung der Agenten. Nach dem NSA-Skandal gab die Affäre Giroud somit den Gegnern des neuen Nachrichtendienstgesetzes weitere Argumente in die Hand. [4]

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. [5]

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. [6]

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. [7]

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. [8]

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. [9]

Institutionen und Volksrechte

Organisation der Bundesrechtspflege

ANDERES
DATUM: 15.10.2011
MARC BÜHLMANN

In die Schlagzeilen geriet die Bundesanwaltschaft aufgrund des Einsatzes so genannter **Trojaner**, also versteckter Software-Programme, die ein Ausspionieren von Computern ermöglichen. Solche Spionage-Software soll in vier Fällen zum Einsatz gekommen sein, dreimal in der Terrorismusbekämpfung und einmal gegen organisierte Kriminalität. [10]

Bildung, Kultur und Medien

Medien

Neue Medien

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. [11]

---

1) NZZ, 4.10.12; Presse vom 28.9, 1., 5. Und 17.10.12.
2) Informatiksicherheit im Nachrichtendienst des Bundes. Bericht der Geschäftsprüfungsdelegation (Zusammenfassung); NZZ, 2.5. und 2.11.13
3) Lagebericht 2014 des NDB; Medienmitteilung VBS vom 5.5.14
4) Presse vom 13.6.14 / NZZ, 14.6., 16.6., 19.6.14 / TA, 17.6., 27.6., 18.9.14.
5) Erläuternder Bericht zum Entwurf eines Bundesgesetzes über die Informationssicherheit; Vernehmlassungsbericht Informationssicherheitsgesetz
6) AB SR, 2017, S. 842 ff.; BBl, 2017, S. 2359 ff.
7) AB NR, 2018, S. 377 ff.
8) AB SR, 2018, S. 767 f.; BaZ, 27.9.18
9) Medienmitteilung SiK-NR vom 9.10.18; NZZ, 10.10.18
10) Presse vom 15.10.11.
11) AB NR, 2009, S. 1005.