

# Ausgewählte Beiträge zur Schweizer Politik

Suchabfrage	<b>24.04.2024</b>
Thema	<b>Keine Einschränkung</b>
Schlagworte	<b>Cyberkriminalität</b>
Akteure	<b>Keine Einschränkung</b>
Prozesstypen	<b>Postulat</b>
Datum	<b>01.01.1965 - 01.01.2021</b>

# Impressum

## Herausgeber

Année Politique Suisse  
Institut für Politikwissenschaft  
Universität Bern  
Fabrikstrasse 8  
CH-3012 Bern  
[www.anneepolitique.swiss](http://www.anneepolitique.swiss)

## Beiträge von

Ackermann, Marco  
Ackermann, Nadja  
Ehrensperger, Elisabeth  
Frick, Karin  
Porcellana, Diane  
Schnyder, Sébastien  
Schubiger, Maximilian  
Schär, Suzanne

## Bevorzugte Zitierweise

Ackermann, Marco; Ackermann, Nadja; Ehrensperger, Elisabeth; Frick, Karin; Porcellana, Diane; Schnyder, Sébastien; Schubiger, Maximilian; Schär, Suzanne 2024. *Ausgewählte Beiträge zur Schweizer Politik: Cyberkriminalität, Postulat, 2000 – 2020*. Bern: Année Politique Suisse, Institut für Politikwissenschaft, Universität Bern.  
[www.anneepolitique.swiss](http://www.anneepolitique.swiss), abgerufen am 24.04.2024.

# Inhaltsverzeichnis

<b>Allgemeine Chronik</b>	1
<b>Grundlagen der Staatsordnung</b>	1
Rechtsordnung	1
Äussere Sicherheit	2
Datenschutz und Statistik	3
Innere Sicherheit	3
Kriminalität	4
<b>Landesverteidigung</b>	4
Landesverteidigung und Gesellschaft	4
Militärorganisation	4
<b>Infrastruktur und Lebensraum</b>	5
Energie	5
Netz und Vertrieb	5
Verkehr und Kommunikation	5
Post und Telekommunikation	5
<b>Bildung, Kultur und Medien</b>	5
Medien	5
Neue Medien	5

## Abkürzungsverzeichnis

<b>EFD</b>	Eidgenössisches Finanzdepartement
<b>VBS</b>	Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport
<b>SiK-NR</b>	Sicherheitspolitische Kommission des Nationalrates
<b>IKT</b>	Informations- und Kommunikationstechnologien
<b>NCS</b>	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken

---

<b>DFF</b>	Département fédéral des finances
<b>DDPS</b>	Département fédéral de la défense, de la protection de la population et des sports
<b>CPS-CN</b>	Commission de la politique de sécurité du Conseil national
<b>TIC</b>	Technologies de l'information et de la communication
<b>SNPC</b>	Stratégie nationale de protection de la Suisse contre les cyberrisques

# Allgemeine Chronik

## Grundlagen der Staatsordnung

### Rechtsordnung

#### Rechtsordnung

POSTULAT  
DATUM: 28.11.2019  
DIANE PORCELLANA

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

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

POSTULAT  
DATUM: 28.11.2019  
DIANE PORCELLANA

Le Conseil fédéral a présenté son **concept global de protection et de défense du cyberspace civil et militaire**, dans son rapport sur l'organisation de la Confédération pour la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques. Une organisation supradépartementale a été privilégiée pour assumer les tâches de cybersécurité, de cyberdéfense et pour la poursuite pénale de la cybercriminalité. Le soutien de l'armée lors de cyberincidents et le déroulement de ses interventions doit encore être défini avec les autorités civiles. Pour assurer la mise en œuvre de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022, les ressources financières ont été augmentées et une soixantaine de postes de travail supplémentaires ont été créés. Enfin, en comparaison internationale, la Suisse possède des structures dans le domaine de la cybersécurité similaires à celles de plusieurs autres pays. Aucun des pays étudiés, à savoir l'Allemagne, la Finlande, la France, Israël, l'Italie et les Pays-Bas, ne possède une organisation unique pour la réalisation des travaux liés aux cyberrisques et n'a confié à son armée la responsabilité d'assurer la protection contre ce type de danger.<sup>2</sup>

POSTULAT  
DATUM: 14.09.2020  
DIANE PORCELLANA

Sur proposition de la CPS-CN, le **Conseil national a refusé de classer les postulats relatifs à la protection contre les cyberrisques** (Po. 18.3003 et 16.4073). La commission ne souhaitait pas les voir classer, car ils sont en cours de mise en œuvre et de nombreuses questions restent encore sans réponse s'agissant de la Stratégie nationale de protection de la Suisse contre les cyberrisques.<sup>3</sup>

## 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.<sup>4</sup>

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 Kompetenzverteilung, 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 Nationalrätinnen 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 auseinandergesetzt. 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.<sup>5</sup>

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 sicherheitspolitische 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.<sup>6</sup>

## Datenschutz und Statistik

POSTULAT  
DATUM: 21.06.2019  
KARIN FRICK

**Mit dem Internet verbundene Produkte** – etwa «smarte» Haushaltsgeräte, Spielzeuge oder Fahrzeuge und digitale Heimassistenten wie «Siri» oder «Alexa» – erfassen und übermitteln individuelle Daten über ihre Nutzerinnen und Nutzer. Diese Daten seien oft schlecht gesichert und leichte Beute für eine zweckentfremdete Nutzung, stellte Nationalrat Mathias Reynard (sp, VS) fest. Sein Postulat mit dem Auftrag, zu prüfen, wie der **Datenschutz** in diesem Bereich verbessert werden könnte, überwies die grosse Kammer in der Sommersession 2019 stillschweigend. Der Bundesrat hatte die Annahme des Postulats beantragt, weil er den Auftrag zusammen mit einem bereits 2017 überwiesenen Postulat Glättli (gp, ZH; Po. 17.4295) erfüllen könne.<sup>7</sup>

## Innere Sicherheit

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.<sup>8</sup>

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.<sup>9</sup>

POSTULAT  
DATUM: 21.06.2019  
MAXIMILIAN SCHUBIGER

«**Haben wir die Hard- und Softwarekomponenten bei unseren kritischen Infrastrukturen im Griff?**», fragte Marcel Dobler (fdp, SG) mit einem im Frühjahr 2019 eingereichten Postulat. Damit griff Dobler Sorgen auf, die bei grösseren IT-Beschaffungen immer wieder geäussert werden. Unter anderem geht es dabei namentlich um ICT-Systeme, die in diversen sensiblen Bereichen eingesetzt werden und die von ausländischen Herstellern produziert und bereitgestellt werden. Solche «digitale[n] Lieferobjekte», die in ihrer Komplexität zu Cyberrisiken führen können, stehen im Fokus seines Vorstosses. Der Bundesrat sollte folglich beauftragt werden, zu prüfen, ob und wie nationale und internationale Standards angewendet werden können, um die Risiken zu vermindern.

Der Bundesrat zeigte sich mit der Stossrichtung des Postulats einverstanden und beantragte dessen Annahme, jedoch seien die Forderungen in einen Bericht aufzunehmen, der bereits mit der Annahme zweier anderer Postulate (Po. 18.3376 und Po. 18.3233) in Auftrag gegeben worden war, erklärte er.

Der Nationalrat sollte sich in der Sommersession 2019 damit befassen, da jedoch auf jegliche Wortmeldungen verzichtet wurde, überwies der Rat das Postulat stillschweigend.<sup>10</sup>

## Kriminalität

**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 Bégli (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.<sup>11</sup>

**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 angebotenen 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.<sup>12</sup>

## Landesverteidigung

### Landesverteidigung

**POSTULAT**  
DATUM: 21.06.2019  
DIANE PORCELLANA

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

Dans sa réponse, le Conseil fédéral proposait d'accepter le postulat, pour que la sécurité soit contrôlée lors des acquisitions.<sup>13</sup>

### 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.<sup>14</sup>

### 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; Armeeinghörigen 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.<sup>15</sup>

## Infrastruktur und Lebensraum

### Energie

#### Netz und Vertrieb

**POSTULAT**  
DATUM: 14.09.2020  
MARCO ACKERMANN

Im Rahmen des Berichts des Bundesrates über Motionen und Postulate der eidgenössischen Räte 2019 schrieb der Nationalrat im September 2020 das Postulat Graf-Litscher (sp, TG) zur **Ausgestaltung einer Meldepflicht bei schwerwiegenden Sicherheitsvorfällen bei kritischen Infrastrukturen** stillschweigend ab. Im November desselben Jahres nahm die SiK-NR bei Beratungen zur Cybersicherheit Kenntnis vom Bericht.<sup>16</sup>

### Verkehr und Kommunikation

#### Post und Telekommunikation

**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).<sup>17</sup>

## Bildung, Kultur und Medien

### Medien

#### Neue Medien

**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 Polizeikörpern überhaupt nicht machbar.<sup>18</sup>

**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 staatschützerischen 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.<sup>19</sup>

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

2) Rapport CF du 27.11.19

3) BO CN, 2020, p.1483 s

- 4) AB SR, 2015, S. 128 f.
- 5) AB NR, 2018, S. 87 f.; NZZ, 3.3.18
- 6) AB NR, 2018, S. 210 f.
- 7) AB NR, 2019, S. 1325; Po. 19.3199
- 8) AB NR, 2011, S. 531; SoS, 5.11.11
- 9) AB NR, 2011, S. 531
- 10) AB NR, 2019, S. 1324
- 11) AB NR, 2016, S. 1801
- 12) AB NR, 2018, S. 535; Po. 17.4295
- 13) BO CN, 2019, p.1324
- 14) BO CE, 2010, p. 550.
- 15) AB NR, 2017, S. 1196
- 16) BBl, 2020, S. 3380; Medienmitteilung SiK-NR vom 17.11.2020
- 17) AB NR, 2011, S. 531, 2266.
- 18) AB NR, 2000, S. 1605.; NZZ, 28.11.00.
- 19) AB SR, 2010, S. 550.