

Sélection d'article sur la politique suisse

Requête	19.04.2024
Thème	Sans restriction
Mot-clés	Cybercriminalité
Acteurs	Sans restriction
Type de processus	Postulat
Date	01.01.1965 - 01.01.2022

Imprimer

Éditeur

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

Contributions de

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

Citations préféré

Ackermann, Marco; Ackermann, Nadja; Ehrensperger, Elisabeth; Frick, Karin; Porcellana, Diane; Schmid, Catalina; Schnyder, Sébastien; Schubiger, Maximilian; Schär, Suzanne 2024. *Sélection d'article sur la politique suisse: Cybercriminalité, Postulat, 2000 - 2021*. Bern: Année Politique Suisse, Institut de science politique, Université de Berne. www.anneepolitique.swiss, téléchargé le 19.04.2024.

Sommaire

Chronique générale	1
Eléments du système politique	1
Ordre juridique	1
Sécurité extérieure	2
Droit pénal	3
Protection des données et statistique	3
Sécurité intérieure	3
Criminalité	4
Armée	5
Armée et société	6
Organisation militaire	6
Infrastructure et environnement	6
Energie	6
Réseau et distribution	6
Transports et communications	6
Poste et télécommunications	6
Enseignement, culture et médias	7
Médias	7
Nouveaux médias	7

Abréviations

EFD	Eidgenössisches Finanzdepartement
VBS	Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport
UNO	Organisation der Vereinten Nationen
SiK-NR	Sicherheitspolitische Kommission des Nationalrates
RK-NR	Kommission für Rechtsfragen des Nationalrats
StGB	Schweizerisches Strafgesetzbuch
IKT	Informations- und Kommunikationstechnologien
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
Fedpol	Bundesamt für Polizei

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
CPS-CN	Commission de la politique de sécurité du Conseil national
CAJ-CN	Commission des affaires juridiques du Conseil national
CP	Code pénal suisse
TIC	Technologies de l'information et de la communication
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
Fedpol	Office fédéral de la police

Chronique générale

Eléments du système politique

Ordre juridique

Ordre juridique

POSTULAT
DATE: 28.11.2019
DIANE PORCELLANA

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

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

POSTULAT
DATE: 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.²

POSTULAT
DATE: 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.³

Sécurité extérieure

POSTULAT
DATE: 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.⁴

POSTULAT
DATE: 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.⁵

POSTULAT
DATE: 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.⁶

Droit pénal

POSTULAT
DATE: 27.09.2021
CATALINA SCHMID

Im Rahmen der Beratung der parlamentarischen Initiative Suter (sp, AG; Pa.Iv. 20.445) beschloss die RK-NR, ein Postulat für **Ergänzungen des Strafgesetzbuchs betreffend Cybermobbing und digitaler Gewalt** einzureichen. Gegenwärtig enthalte das Strafgesetzbuch zwar verschiedenste Artikel, die zur Bestrafung von Cybermobbing zur Anwendung kommen könnten, allerdings reiche die blosser Erwähnung des Cybermobbings im StGB nicht aus, um die «Nöte der Betroffenen» zu lindern, begründete die Kommission ihren Vorstoss. In der Herbstsession 2021 nahm der Nationalrat das Postulat stillschweigend an.⁷

Protection des données et statistique

POSTULAT
DATE: 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.⁸

POSTULAT
DATE: 19.03.2021
DIANE PORCELLANA

La conseillère nationale Judith Bellaïche (pvl, ZH) charge le Conseil fédéral d'étudier comment le **piratage éthique** pourrait être **institutionnalisé** et encouragé dans l'Administration fédérale et les entreprises liées à la Confédération. Le piratage éthique vise à chercher et détecter les failles, afin de renforcer la sécurité du réseau et des systèmes informatiques. Pour ce faire, il faudrait des directives qui définissent le cadre du piratage éthique, notamment le processus pour détecter les failles de sécurité et les tests de robustesse. Toute poursuite à l'encontre des pirates impliqués dans ce type de piratage doit être exclue. Le Centre national pour la cybersécurité devrait accompagner et soutenir cette démarche.

Le Conseil fédéral a proposé d'accepter le postulat, lequel a été adopté sans discussion par le Conseil national.⁹

Sécurité intérieure

POSTULAT
DATE: 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.¹⁰

POSTULAT
DATE: 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.¹¹

POSTULAT
DATE: 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 Cyberisiken 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.¹²

Criminalité

POSTULAT
DATE: 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 Bégulé (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.¹³

POSTULAT
DATE: 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.¹⁴

POSTULAT
DATE: 10.06.2021
DIANE PORCELLANA

Comme le Conseil fédéral a rendu 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), l'Assemblée fédérale classe donc le postulat.

POSTULAT
DATE: 10.06.2021
KARIN FRICK

Der Nationalrat schrieb das Postulat Glättli (gp, ZH) zur **Prüfung von Sicherheitsstandards für Internet-of-Things-Geräte** in der Sommersession 2021 ab, nachdem es der Bundesrat mit einem Bericht erfüllt hatte.¹⁵

POSTULAT
DATE: 21.09.2021
CATALINA SCHMID

Mittels Postulat forderte SP-Nationalrätin Yvonne Feri (AG) vom Bundesrat die Ausarbeitung eines Berichts zur Frage, was das **Fedpol gegen die sexuelle Gewalt an Kindern im Internet unternimmt**. Konkret sollen der Umgang mit Verdachtsfällen aus dem In- und Ausland, eine nationale Online-Meldestelle sowie die notwendigen Mittel und Massnahmen zur Wahrnehmung und Bekämpfung von Pädokriminalität geprüft werden. Ihren Vorstoss begründete die PostulantIn einerseits mit der steigenden Zahl der sexuellen Belästigungen an Kindern im Internet und andererseits mit dem Scheitern

einer wirksamen Bekämpfung der Cyberpädokriminalität in der Schweiz. Letzteres sei darauf zurückzuführen, dass die dazu notwendigen personellen und technischen Ressourcen auf Bundes- und Kantonebene knapp seien und sich die Gesetzgebung auf Kantonsgebiete beschränke, obschon das Internet keine geografischen Grenzen kenne. Da viele Verdachtsfälle aus dem Ausland kämen, triagiert und den jeweiligen Kantonen zugewiesen werden müssten, komme dem Fedpol als Schnittstelle zwischen dem Ausland und den Kantonen eine wichtige Rolle zur Bekämpfung der Cyberpädokriminalität zu. Die Stärkung des Fedpol in dieser Rolle sei somit notwendig. Wie Justizministerin Karin Keller-Sutter im Ratsplenum erklärte, liege die Strafverfolgung von Pädokriminalität in der Zuständigkeit der Kantone. Das Fedpol nehme als Zentralstelle nur die Rolle des Koordinators ein und verfolge Verdachtsfälle seit Beginn des Jahres nicht mehr selbst. Der Bundesrat sei der Ansicht, dass die bestehende Rollen- und Aufgabenteilung zwischen Bund und Kantonen eine wirksame Bekämpfung der Cyberpädokriminalität auf nationaler und internationaler Ebene gewährleisten könne und beantragte deshalb die Ablehnung des Postulats. In der Herbstsession 2021 hiess der Nationalrat das Postulat entgegen dem Antrag des Bundesrats mit 127 zu 62 Stimmen gut.¹⁶

POSTULAT
DATE: 21.09.2021
CATALINA SCHMID

Die Fallzahlen von Cyberpädokriminalität stiegen seit Jahren an und befanden sich gegenwärtig «auf einem Allzeithoch», so die Schätzungen des FBI und der UNO. Diese Erkenntnis veranlasste Fabio Regazzi (cvp, TI) im Jahr 2019 dazu, mittels Postulat eine Prüfung von rechtlichen und sonstigen **Massnahmen zur Bekämpfung von sexuellem Missbrauch von Kindern via Live-Streaming** zu fordern. Als mögliche Massnahme solle insbesondere der Einsatz von computergenerierten, künstlichen Bildern von Kindern zur Anlockung potenzieller Täter geprüft werden. Dieser Ansatz habe sich in den Niederlanden bereits seit 2014 als sehr effizient und wirksam entpuppt, sodass auch Deutschland vorhabe, diesen künftig einzusetzen. Der Bundesrat sei sich der – durch die Covid-19-Pandemie noch zusätzlich verstärkten – Zunahme von Pädokriminalität im Internet und der deshalb grossen Relevanz von deren Bekämpfung sehr bewusst, unterstrich Justizministerin Karin Keller-Sutter im September 2021 im Ratsplenum. Die Bekämpfung von Pädokriminalität liege jedoch grundsätzlich in der Zuständigkeit der Kantone, dies insbesondere seit der Rückübertragung bestimmter Aufgaben vom Bund an die Kantone zu Beginn des Jahres 2021. Der Bundesrat vertrat die Meinung, dass diese Rollenverteilung effizient und wirksam im Kampf gegen die Pädokriminalität sei und dass daran festgehalten werden müsse. Aus diesem Grund beantragte er die Ablehnung des Postulats. Der Nationalrat nahm das Postulat Regazzi in der Herbstsession 2021 entgegen diesem Antrag mit 146 zu 37 Stimmen bei 4 Enthaltungen an. Die Zustimmung zum Postulat war parteilich breit abgestützt und vereinte vorwiegend Nationalrätinnen und -räte der Grünen, der SP, der Mitte und der SVP. Die Grünliberalen und die FDP lehnten das Postulat grösstenteils ab.¹⁷

Armée

Armée

POSTULAT
DATE: 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.¹⁸

POSTULAT
DATE: 17.12.2021
DIANE PORCELLANA

Le Conseil national a adopté, sans discussion, le postulat déposé par Judith Bellaïche (pvl, ZH) intitulé **Cyberrisques dans l'espace**. Le Conseil fédéral est donc chargé de présenter la situation de la Suisse face à la numérisation croissante de l'espace et aux cyberrisques y relatifs. L'espace étant de plus en plus utilisé pour la transmission de données à des fins étatiques et commerciales, des milliers de satellites seront en orbite dans les années à venir. Pour optimiser la situation de la Suisse vis-à-vis de la dépendance aux satellites étrangers, le Conseil fédéral se saisira de la question de la dépendance et de la sécurité des données étatiques et privées. Le Conseil fédéral proposait d'accepter le postulat.¹⁹

Armée et société

POSTULAT
DATE: 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.²⁰

Organisation militaire

POSTULAT
DATE: 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; Armeeingehörigen 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.²¹

Infrastructure et environnement

Energie

Réseau et distribution

POSTULAT
DATE: 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.²²

Transports et communications

Poste et télécommunications

POSTULAT
DATE: 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).²³

Enseignement, culture et médias

Médias

Nouveaux médias

POSTULAT

DATE: 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.²⁴

POSTULAT

DATE: 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.²⁵

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, 2021, S. 1935; Po. 21.3969

8) AB NR, 2019, S. 1325; Po. 19.3199

9) BO CN, 2021, p. 662

10) AB NR, 2011, S. 531; SoS, 5.11.11

11) AB NR, 2011, S. 531

12) AB NR, 2019, S. 1324

13) AB NR, 2016, S. 1801

14) AB NR, 2018, S. 535; Po. 17.4295

15) BBI, 2021 747; Po. 17.4295

16) AB NR, 2021, S. 1741; Po. 19.4016

17) AB NR, 2021, S. 1746 f.; Po. 19.4105

18) BO CN, 2019, p.1324

19) BO CN, 2021, p. 2711

20) BO CE, 2010, p. 550.

21) AB NR, 2017, S. 1196

22) BBI, 2020, S. 3380; Medienmitteilung SiK-NR vom 17.11.2020

23) AB NR, 2011, S. 531, 2266.

24) AB NR, 2000, S. 1605.; NZZ, 28.11.00.

25) AB SR, 2010, S. 550.