année politique suisse

DOKUMENTATION · ANALYSE · DIFFUSION

Ausgewählte Beiträge zur Schweizer Politik

Suchabfrage	**23.04.2024**
Thema	**Landesverteidigung**
Schlagworte	**Datenschutz, Gesellschaftsrecht**
Akteure	**Keine Einschränkung**
Prozesstypen	**Keine Einschränkung**
Datum	**01.01.1965 - 01.01.2023**

Impressum

Herausgeber

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

Beiträge von

Magnin, Chloé
Porcellana, Diane
Schubiger, Maximilian

Bevorzugte Zitierweise

Magnin, Chloé; Porcellana, Diane; Schubiger, Maximilian 2024. *Ausgewählte Beiträge zur Schweizer Politik: Landesverteidigung, Datenschutz, Gesellschaftsrecht, 2015 - 2022*. Bern: Année Politique Suisse, Institut für Politikwissenschaft, Universität Bern. www.anneepolitique.swiss, abgerufen am 23.04.2024.

Inhaltsverzeichnis

Abkürzungsverzeichnis

EFD	Eidgenössisches Finanzdepartement
VBS	Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport
SiK-SR	Sicherheitspolitische Kommission des Ständerates
EU	Europäische Union
ISB	Informatiksteuerungsorgan des Bundes
MELANI	Melde- und Analysestelle Informationssicherheit
WEA	Weiterentwicklung der Armee
NDB	Nachrichtendienst des Bundes (bis 2010: Strategischer Nachrichtendienst und Dienst für Analyse und Prävention)
MIG	Bundesgesetz über die militärischen Informationssysteme
NCSC	Nationales Zentrum für Cybersicherheit

DFF	Département fédéral des finances
DDPS	Département fédéral de la défense, de la protection de la population et des sports
CPS-CE	Commission de la politique de sécurité du Conseil des Etats
UE	Union européenne
UPIC	Unité de pilotage informatique de la Confédération
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
DEVA	Développement de l'armée
SRC	Service de renseignement de la Confédération (à 2010: Service de renseignement stratégique et Service d'analyse et de prévention)
LSIA	Loi fédérale sur les systèmes d'information de l'armée
NCSC	Centre national pour la cybersécurité

Allgemeine Chronik

Landesverteidigung

Landesverteidigung

BUNDESRATSGESCHÄFT
DATUM: 24.11.2021
CHLOÉ MAGNIN

En raison du DEVA, les structures et le fonctionnement de l'administration militaire ont considérablement évolué. Les nouveaux besoins de l'armée en ce qui concerne le traitement des données personnelles n'étant pas compris dans la base légale actuelle, le Conseil fédéral demande une **révision de la loi fédérale sur les systèmes d'information de l'armée**. En effet, afin de traiter les données personnelles de manière optimale, une adaptation de la LSIA est nécessaire. Cette modification concerne principalement le traitement et la collecte de données personnelles sans toutefois conduire à recueillir des informations supplémentaires.
Le premier mars 2022, la modification de la loi a été acceptée à l'unanimité par le Conseil des États. [1]

PARLAMENTARISCHE INITIATIVE
DATUM: 06.12.2021
CHLOÉ MAGNIN

Alors que la sécurité nationale est au centre des discussions depuis la fin de l'année 2021 – nombreuses cyberattaques, éclatement de la guerre en Ukraine depuis février 2022 –, une initiative parlementaire du conseiller aux États Charles Juillard (centre, JU), lancée fin 2021 rappelle que ce thème est une préoccupation avérée. En effet, avec l'objet **«Cybersécurité. Mettre en place une infrastructure numérique souveraine et des standards de sécurité de gouvernance»**, le sénateur jurassien espère convaincre qu'un virage est à prendre et qu'une collaboration entre les différents acteurs suisses – privés et publics – est nécessaire afin de protéger le pays contre les différentes menaces qui existent au temps du numérique. Le but est ainsi de renforcer la cybersécurité du pays et de favoriser une unité du système de données sur l'ensemble du territoire, notamment par la création d'un «cloud souverain» qui rassemblera l'ensemble de ces dernières. Si l'objet est accepté, la Confédération sera à la tête des opérations et prendra en charge le financement du projet. [2]

POSTULAT
DATUM: 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. [3]

BUNDESRATSGESCHÄFT
DATUM: 17.06.2022
CHLOÉ MAGNIN

Après sa modification par le Conseil des États en mars 2022, le texte est validé par les deux Conseils trois mois plus tard. A la mi-juin, le texte final a passé avec succès l'épreuve du **vote final**. Au Conseil national, il a été adopté par 192 voix contre 1 (4 abstentions) et au Conseil des États, son adoption a été unanime. La date limite pour un référendum est fixée au 6 octobre 2022. Jusque-là, les débats sont clos. [4]

PARLAMENTARISCHE INITIATIVE
DATUM: 19.08.2022
CHLOÉ MAGNIN

L'**initiative parlementaire** déposée par Charles Juillard (centre, JU) a été traitée en même temps que l'objet 21.495 par la CPS-CE. Des conclusions similaires ont été tirées. De ce fait, le **rejet** a été **proposé** par 6 voix contre 2 et une abstention. Une nouvelle initiative pourrait voir le jour, après réévaluation du dossier, car la commission soutient le but visé par l'initiative parlementaire mais pas la manière de l'atteindre. [5]

BUNDESRATSGESCHÄFT
DATUM: 02.12.2022
CHLOÉ MAGNIN

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

En 2016, après l'acceptation par l'EU d'une directive concernant le signalement des cyberattaques visant les infrastructures critiques et de discussions internes, la Suisse a chargé le département fédéral des finances (DFF) de fournir, d'ici fin 2021, les bases légales pour introduire une obligation de signaler les cyberattaques contre les infrastructures critiques, dont le secteur bancaire, l'armée, le système de soins médicaux ou encore les infrastructures relatives au transport routier. Cette analyse a également révélé des manquements au niveau du centre national pour la cybersécurité (NCSC). C'est pourquoi une partie du projet final est réservée à la spécification des tâches assignées au NCSC. En cas de cyberattaques concernant les infrastructures critiques suisses, le NCSC devra réceptionner les signalements obligatoires mais aussi les signalements volontaires pour permettre à la Confédération d'avoir une vue d'ensemble sur les failles du système.

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

Finalement, le Conseil fédéral a fait attention à ce que le projet final repose sur des procédures simples, que les signalements soient récompensés par un service de conseil assuré par le NCSC, et que le non-respect des conditions soit puni par une sanction pécuniaire pouvant s'élever jusqu'à CHF 100'000, dont CHF 20'000 directement à la charge de l'entreprise exploitant l'infrastructure critique concernée. Toutefois, le Conseil fédéral estime que cette dernière mesure restera symbolique en raison d'une collaboration de longue date entre les infrastructures critiques et le gouvernement. [6]

Landesverteidigung und Gesellschaft

STUDIEN / STATISTIKEN
DATUM: 01.01.2015
MAXIMILIAN SCHUBIGER

Die Militärakademie der ETH hat 2015 wiederum zusammen mit dem Center for Security Studies die **Jahresstudie „Sicherheit"** publiziert. Die Autorinnen und Autoren stellten auch in diesem Jahr ein grundlegendes Gefühl der Sicherheit in der Schweizer Bevölkerung fest. Angst vor Bedrohungen wurde nur in geringem Mass erkannt und wenn, dann im Bereich der Datensicherheit oder bezüglich Cyber-Angriffen. Die Frage nach der Notwendigkeit der Armee wurde mit sehr hoher Zustimmung beantwortet und sogar die jüngste Alterskohorte befürwortete die Armee so deutlich wie noch nie in der dreissigjährigen Messperiode. Diese jüngeren Respondenten wiesen in dieser Periode einen Anstieg um 8 Prozentpunkte aus (74%; 2014: 66%). Insgesamt wurde auch das Modell der Milizarmee deutlich bejaht und einer reinen Berufsarmee vorgezogen, wobei bezüglich alternativer Dienstmodelle ambivalente Erkenntnisse gezogen werden mussten: Einerseits erhielt eine obligatorische Wehrpflicht nur für Männer eine hohe Zustimmung, andererseits sprachen sich ebenso viele Befragte gegen eine Umwandlung in eine obligatorische Dienstpflicht aus. Es konnten keine eindeutigen Schlüsse gezogen werden, ob ein Modell mit einer Dienstpflicht, die die Frauen mit einschliesst, auf Zustimmung stossen würde. Eine Wehrpflicht unter Miteinbezug weiblicher Dienstleistenden wurde mehrheitlich abgelehnt, so auch bezüglich der Ausweitung der Dienstpflicht für Ausländer. Einwohner ohne schweizerische Staatsbürgerschaft sollen gemäss dieser Meinungsumfrage auch nicht in den Zivil-, oder einen allfälligen Sozialdienst rekrutiert werden.
Bezüglich der Zufriedenheit mit der Armee wurde keine Veränderung gegenüber dem Vorjahr registriert. Sie verharrt auf durchschnittlich 6.3 Punkten auf einer Zehnerskala zwischen "überhaupt nicht zufrieden" und "sehr zufrieden". Was die Abschaffung der Wehrpflicht angeht, sprachen sich in der Selbsteinschätzung links Eingestellte und

höher Gebildete stärker für eine solche aus. Weniger Gebildete und sich auf der Links-Rechts-Achse eher rechts einstufende Befragte stützten die Wehrpflicht hingegen eher. Insgesamt ist die Zustimmung zur Abschaffung der Wehrpflicht gegenüber dem Vorjahr um einen Prozentpunkt auf 38% gestiegen. Abnehmend hingegen ist die Haltung, dass die Schweiz zu viel für die Verteidigung ausgebe. Dies empfanden noch 33% der Befragten (-4 Prozentpunkte). Dass dagegen mehr ausgegeben werden sollte, gaben 16% an, was einer pointierten Steigerung um 7 Prozentpunkte bedeutet. Die Milizarmee als Dienstmodell wird von einer Mehrheit von 58% gutgeheissen (-3 Prozentpunkte), dies bedeutet den dritthöchsten Wert seit 1995. Die dienstpflichtige Kohorte der jüngeren Befragten (20–29-jährige) zeigte sich einer Berufsarmee deutlich stärker zugetan als noch im Vorjahr (48%, + 5 Prozentpunkte). Die Bevölkerung fühle sich sehr sicher und schaue zuversichtlich in die Zukunft, schlossen die Herausgeber der Studie. [7]

Militärorganisation

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. [8]

1) BO, CE, 2022, p.33 f.; FF, 2021 3046
2) Iv.pa. 21.507; Exp, 5.4.22; 24H, 6.4.22; NZZ, 30.4.22
3) BO CN, 2021, p. 2711
4) BO CN, 2022; BO, CE, 2022; FF, 2022 1565
5) Communiqué de presse CPS-CE du 22.2.22; Communiqué de presse CSP-CN du 19.8.22
6) FF, 2023 84
7) Jahresstudie Sicherheit 2015

8) Aktionsplan Cyberdefence