année politique suisse

DOKUMENTATION · ANALYSE · DIFFUSION

Ausgewählte Beiträge zur Schweizer Politik

Suchabfrage	**24.04.2024**
Thema	**Landesverteidigung**
Schlagworte	**Cyberkriminalität**
Akteure	**Keine Einschränkung**
Prozesstypen	**Keine Einschränkung**
Datum	**01.01.1965 - 01.01.2024**

Impressum

Herausgeber

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

Beiträge von

Magnin, Chloé
Porcellana, Diane
Schnyder, Sébastien
Schubiger, Maximilian

Bevorzugte Zitierweise

Magnin, Chloé; Porcellana, Diane; Schnyder, Sébastien; Schubiger, Maximilian 2024. *Ausgewählte Beiträge zur Schweizer Politik: Landesverteidigung, Cyberkriminalität, 2010 - 2023*. Bern: Année Politique Suisse, Institut für Politikwissenschaft, Universität Bern. www.anneepolitique.swiss, abgerufen am 24.04.2024.

Inhaltsverzeichnis

Abkürzungsverzeichnis

EFD	Eidgenössisches Finanzdepartement
VBS	Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport
BAFU	Bundesamt für Umwelt
SiK-SR	Sicherheitspolitische Kommission des Ständerates
ETH	Eidgenössische Technische Hochschule
SiK-NR	Sicherheitspolitische Kommission des Nationalrates
EU	Europäische Union
ISB	Informatiksteuerungsorgan des Bundes
MELANI	Melde- und Analysestelle Informationssicherheit
IKT	Informations- und Kommunikationstechnologien
WEA	Weiterentwicklung der Armee
BZG	Bevölkerungs- und Zivilschutzgesetz
NATO	North Atlantic Treaty Organization
GSoA	Gruppe für eine Schweiz ohne Armee
MG	Bundesgesetz über die Armee und die Militärverwaltung (Militärgesetz)
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
ZDG	Bundesgesetz über den zivilen Ersatzdienst (Zivildienstgesetz)
NDB	Nachrichtendienst des Bundes (bis 2010: Strategischer Nachrichtendienst und Dienst für Analyse und Prävention)
AO	Verordnung der Bundesversammlung über die Organisation der Armee
CYD	Cyber-Defence Campus
NCSC	Nationales Zentrum für Cybersicherheit
NTC	Nationales Testinstitut für Cybersicherheit
ISG	Informationssicherheitsgesetz

DFF	Département fédéral des finances
DDPS	Département fédéral de la défense, de la protection de la population et des sports
OFEV	Office fédéral de l'environnement
CPS-CE	Commission de la politique de sécurité du Conseil des Etats
EPF	École polytechnique fédérale
CPS-CN	Commission de la politique de sécurité du Conseil national
UE	Union européenne
UPIC	Unité de pilotage informatique de la Confédération
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
TIC	Technologies de l'information et de la communication
DEVA	Développement de l'armée
LPPCi	Loi sur la protection de la population et sur la protection civile
OTAN	L'Organisation du traité de l'Atlantique nord
GSsA	Groupe pour une Suisse sans Armée
LAAM	Loi fédérale sur l'armée et l'administration militaire (Loi sur l'armée)
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
LSC	Loi fédérale sur le service civil
SRC	Service de renseignement de la Confédération (à 2010: Service de renseignement stratégique et Service d'analyse et de prévention)
OOrgA	Ordonnance de l'Assemblée fédérale sur l'organisation de l'armée
CYD	Campus cyberdéfense
NCSC	Centre national pour la cybersécurité
NTC	Institut national de test pour la cybersécurité
LSI	Loi fédérale sur la sécurité de l'information

Allgemeine Chronik

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. [1]

BERICHT
DATUM: 31.12.2019
DIANE PORCELLANA

Rétrospective annuelle 2019: Armée

Durant l'année 2019, la refonte du **système de l'obligation de servir** était au centre des discussions dans l'arène politique et médiatique. En février, le Conseil fédéral avait présenté dans son projet d'adaptation de la loi sur le service civil (LSC), huit mesures pour durcir les conditions d'accès au service civil, qui ont été fortement critiquées par les milieux de gauche et les établissements d'affectation. Le Conseil des Etats, suivant l'avis de sa commission, n'a juste pas approuvé l'interdiction des affectations à l'étranger. Contrairement à sa consœur, la CPS-CN a proposé au Conseil national de soutenir l'ensemble des mesures.
En parallèle, dans le cadre de la révision totale de la loi sur la protection de la population et sur la protection civile (LPPCi), le Parlement n'a pas souhaité introduire un service long pour la protection civile, ni reconnaître le service civil comme une organisation partenaire œuvrant dans le cadre de la protection de la population. Après conciliation, il a été décidé d'affecter les contributions de remplacement pour la rénovation d'abris privés et publics, et non pas pour couvrir les coûts occasionnés après la construction d'abris privés.
Quand bien même les révisions du système de l'obligation de servir étaient en cours, le dépôt d'une initiative populaire pour une obligation universelle de servir l'intérêt général a été annoncée pour 2020. Le Conseil fédéral a d'ailleurs été chargé d'approfondir les modalités et les implications du modèle du service citoyen (Po. 19.3735). Dans la presse, Philippe Rebord, actuel chef de l'Armée, a pour sa part indiqué vouloir autoriser le service militaire pour les personnes transgenres.

Le **renouvellement des moyens de protection de l'espace aérien** a également retenu l'attention. Le Conseil fédéral a décidé de soumettre à l'Assemblée fédérale un arrêté de planification relatif à l'acquisition d'avions de combat, attaquable par référendum, notamment après avoir reçu le rapport de l'astrophysicien et pilote Claude Nicollier. L'attribution de son mandat par la conseillère fédérale Viola Amherd, ainsi que les conclusions de son rapport, ne sont pas passées inaperçues dans les médias. Pour la défense sol-air, le renouvellement s'effectuera dans le cadre du processus normal d'acquisition d'armement. L'enveloppe de 6 milliards de francs a été acceptée par les deux chambres. Toutefois, elles n'ont pas encore réussi à s'accorder sur les affaires compensatoires. En premier lieu, le Conseil des Etats exigeait une compensation intégrale de la valeur contractuelle, alors qu'une compensation à hauteur de 60% suffisait pour le Conseil national. Dans un second temps, la chambre des cantons a accepté une compensation de 80%. Si l'acquisition de nouveaux avions de combat n'est pas encore certaine – le GSsA a déjà brandi la menace d'un référendum –, l'armée dispose toutefois dans ses rangs, pour la première fois, d'une femme pilote de chasse.
Pour se prémunir contre les menaces dans le domaine de la cybercriminalité, la Suisse peut également compter, depuis cette année, sur le campus cyberdéfense.

Dans son **message sur l'armée 2019**, le Conseil fédéral a détaillé les différents projets d'arrêtés fédéraux relatifs au programme d'armement, au programme immobilier du DDPS et aux crédits-cadres pour le matériel de l'armée. Il a également soumis une modification de la LAAM, afin de permettre l'octroi d'indemnités financières aux militaires de milice à faire valoir pour des formations civiles.
S'agissant des munitions, ce n'est pas le crédit sollicité dans le message qui a suscité le plus d'intérêt de la part de la population de **Mitholz**, mais la situation de l'ancien dépôt de munitions dans leur village. Les experts mandatés par l'OFEV ont confirmé le risque élevé émanant de l'ouvrage. Quant au groupe de travail «Mitholz», il a recommandé

d'approfondir les options pour une élimination partielle ou complète des munitions. Le Conseil des Etats a rejeté la motion Grossen (pvl, BE; Mo. 18.3798) priant le Conseil fédéral de vider l'entrepôt. Pour l'instant, le Conseil fédéral devra continuer de subventionner, après 2020, l'assainissement des sols contaminés par les tirs historiques et les tirs de campagne.

Au mois d'avril, 4.29% des articles de presse relayaient des informations en lien avec le thème de l'armée. Le salaire du commandant de corps Daniel Baumgartner, futur attaché de défense à Washington, a été vivement critiqué, puisqu'il continuera de toucher son salaire actuel alors qu'il exercera une fonction devant être nettement moins rémunérée. Les médias ont présenté **plusieurs papables pour succéder à Philippe Rebord**, qui avait annoncé, le même mois, sa démission pour des raisons de santé. Thomas Süssli a été nommé pour reprendre les commandes de l'armée.
Enfin, malgré les différentes critiques envers l'institution militaire et ses activités, l'étude «Security 2019» de l'ETH de Zurich révèle une attitude toujours positive de la population vis-à-vis des militaires. L'organisation de l'armée en milice est préférée à une armée purement professionnelle. La satisfaction à l'égard des forces armées a repris cette année, après l'année 2018 marquée par le début de la mise en œuvre du projet de réorganisation de l'armée intitulé «Développement de l'armée» (DEVA). [2]

ANDERES
DATUM: 11.12.2020
DIANE PORCELLANA

L'introduction d'une **obligation de signaler les cyberattaques pour les exploitants d'infrastructures critiques** sera soumise à consultation. Avec cette décision, le Conseil fédéral matérialise la mesure formulée dans la Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022 et fait écho au postulat d'Edith Graf-Litscher (ps, TG). Pour ce faire, le DFF est chargé de soumettre un projet de loi déterminant les types d'incidents à signaler, les délais et les concernés par l'obligation. Les dispositions concrètes relatives à l'obligation de déclarer figureront dans des actes législatifs distincts en fonction de la situation spécifique des secteurs concernés. Si les adaptations législatives devaient être saluées lors de la consultation et approuvées par la suite, les données récoltées dans le cadre de l'obligation permettraient de diffuser des alertes rapides, de renforcer la sécurité et une meilleure évaluation des menaces. [3]

BERICHT
DATUM: 24.11.2021
DIANE PORCELLANA

En exécution des postulats Dobler (19.3135) et (19.3136), le Conseil fédéral a fourni son rapport intitulé «**Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense**». Le rapport détaille les standards existants et les engagements de la Confédération et des exploitant.e.s d'infrastructures critiques y découlant en la matière. Si le domaine de la sécurité des produits est plutôt normé et appliqué, les directives relatives à la gestion des risques de la chaîne d'approvisionnement dans le domaine de la cybersécurité sont moins étoffées. La Confédération dispose d'une base légale pour appliquer les standards de sécurité des produits TIC et la gestion des risques de la chaîne d'approvisionnement. Les règles liées au respect des standards de sécurité des TIC pour les infrastructures critiques sont par contre «rares». Pour les standards de sécurité des produits, le rapport appelle à se concentrer sur la mise en œuvre globale et continue des directives. S'agissant des directives en matière de gestion des risques de la chaîne d'approvisionnement dans le domaine de la cybersécurité, les standards se révèlent être des recommandations plutôt que des normes contraignantes. Afin de remédier au manque de directives contraignantes pour les infrastructures critiques, le rapport expose plusieurs solutions: l'élaboration de directives juridiquement contraignantes, les références aux standards dans le domaine de la sécurité des produits ou des directives adressées aux exploitant.e.s d'infrastructures critiques pour une gestion sûre des produits TIC. Le rapport recommande également d'introduire des directives liées à des mesures régulatrices pour la gestion des risques de la chaîne d'approvisionnement. [4]

BERICHT
DATUM: 24.11.2021
CHLOÉ MAGNIN

Dans une situation politique, environnementale et sanitaire de plus en plus complexe et incertaine, la Confédération helvétique a publié en novembre 2021 son **rapport sur la politique de sécurité 2021**. Afin de garantir la sûreté dont le pays bénéficie actuellement, la Suisse compte poursuivre et même intensifier ses actions dans le domaine de la sécurité nationale. Elle s'est fixé neuf objectifs pour la période à venir, souhaitant ainsi assurer la protection du pays malgré les nombreux changements et évolutions que le monde politique vit en cette période marquée notamment par un déploiement des conflits (hybrides et traditionnels), la pandémie du Covid-19 ou

encore le changement climatique.
Parmi les neufs objectifs que le gouvernement a défini comme prioritaires, on retrouve: (1) Renforcer la détection des menaces afin d'agir aussi tôt que possible; (2) renforcer la coopération internationale dans le but de stabiliser la sécurité; (3) prendre davantage en considération les conflits hybrides, les cyberattaques et la désinformation et adapter les ressources militaires afin de renforcer la sécurité du pays et faire face aux menaces; (4) encourager la formation libre de l'opinion public; (5) renforcer la sécurité contre les cybermenaces; (6) combattre le terrorisme et les autres formes de criminalité; (7) renforcer l'indépendance de la Suisse dans son approvisionnement lors de crises internationales; (8) améliorer la gestion, la prévention et la sécurité en cas de catastrophes ou de situations d'urgence (changement climatique); et (9) renforcer la collaboration entre les différents acteurs de la sécurité suisse (armée, police, gestion des douanes, service civil, etc.).
Afin d'atteindre chacun de ces neuf objectifs, la Confédération helvétique compte sur une coopération efficace et structurée entre les différents domaines politiques et instruments suisses tels que la Confédération, les cantons, les communes, la politique étrangère ou encore l'armée. Ainsi, la politique de sécurité de la Suisse a pu être définie comme étant une «tâche commune». Celle-ci nécessite une collaboration engagée de la part des différents acteurs suisses pour viser la réalisation des desseins fixés par le rapport fédéral. Dans la conclusion de ce dernier, un accent tout particulier est mis sur les révisions de la politique de sécurité suisse. En effet, il est rappelé que toute modification de la politique de sécurité s'appliquant à la gestion du personnel de milice devrait impliquer la Confédération, les cantons et les communes. La confiance du Conseil fédéral en sa capacité à défendre la sécurité du territoire et les habitants est également évoquée.
Il est encore à noter que, lors de la discussion de l'objet au Conseil national, la situation en Europe, actuellement mouvementée en raison de la guerre en Ukraine, a suscité divers avis parmi les parlementaires. Une certaine disparité sur la direction à prendre en terme de politique de sécurité a pu être remarquée entre la gauche et la droite. Dans ce contexte particulier, le Conseil fédéral a annoncé qu'il publiera un complément au rapport d'ici fin 2022. [5]

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. [6]

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. [7]

BERICHT
DATUM: 09.03.2022
CHLOÉ MAGNIN

«Ce qui devait être un exercice tranquille est devenu brûlant d'actualité avec l'invasion de l'Ukraine par l'armée russe» s'est exprimé Fabien Fivaz (verts, NE), dans le cadre des discussions sur le **rapport sur la politique de sécurité 2021**. L'objet a été traité le 9 mars 2022 par le Conseil national et a suscité de nombreuses réactions. Après quelques interventions en début de session, où le contenu du rapport a été mis en évidence, soit pour le féliciter, soit pour le critiquer, diverses prises de parole ont donné suite à des échanges entre les députés et la conseillère fédérale Viola Amherd.

On notera que les avis fondamentaux sur la politique de sécurité suisse **varient énormément entre la droite et la gauche**.
En effet, à **droite**, David Zuberbühler (udc, AR) a critiqué le manque d'ambition du Conseil fédéral. Pour lui, les capacités militaires suisses seraient trop faibles pour réussir à atteindre les objectifs fixés par la Confédération. Lors de son intervention, il a aussi évoqué la «mauvaise option» de vendre l'entreprise fournisseuse de munitions Ruag Ammotec. Pour le vert'libéral François Pointet (pvl, VD), la position soutenue par ses collègues de l'UDC ne constitue pas la solution. C'est pourquoi, au lieu d'une augmentation des effectifs de l'armée, il a mis l'accent sur d'autres éléments: les vert'libéraux prônent une «armée moderne, agile, composée de militaires bien entraînés et complètement équipés de matériel de pointe» ainsi qu'une collaboration forte avec les États voisins. Le parti a été très surpris d'apprendre que le Conseil fédéral n'est pas favorable à la création d'un état-major permanent. Cet organe militaire visant à la sécurité de la population demanderait (notamment) des connaissances techniques trop importantes. Un avis que les vert'libéraux – tout comme la PLR Jacqueline de Quattro (plr, VD) – ne partagent pas. Selon eux, cet outil pourrait être une solution adaptée pour lutter contre les états de crise futures.
La **gauche**, quant à elle, reconnaît la possible menace d'une attaque, mais d'après Priska Seiler Graf (ps, ZH), on ne s'attend pas à ce que des chars russes arrivent à la frontière du Rhin. Le socialiste Pierre-Alain Fridez (ps, JU) a évoqué, en raison de sa position géographique, une situation favorable pour la sécurité de la Suisse: «Paradoxalement, notre sécurité est sans doute renforcée aujourd'hui grâce au réveil de l'OTAN». De manière générale, la gauche a critiqué les dépenses demandées par la droite pour des armes qui ne déjoueraient pas les menaces cyber ou les attaques de missiles auxquelles la Suisse pourrait être sujette. Léonore Porchet (verts, VD) évoque par exemple les dépenses importantes liées aux nouveaux avions de chasse, qu'elle qualifie comme étant un «outil militaire disproportionné et inutile». Pour elle, la plus grande menace pour la Suisse reste le changement climatique et ce nouvel investissement ne permettra pas d'y faire face.
Finalement, tous les partis ont pris note du rapport. Avant les débats en plénum, la commission de la politique de sécurité du Conseil national (CPS-CN) s'était pour sa part prononcée en faveur d'une augmentation du budget de l'armée. Une minorité proposait cependant d'attendre le complément au rapport pour débattre d'une éventuelle augmentation. Ce dernier a été agendé pour fin 2022 par le Conseil fédéral. [8]

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. [9]

MOTION
DATUM: 12.09.2022
CHLOÉ MAGNIN

Alors que le **progrès technologique** incite les entreprises publiques **et** privées à digitaliser leurs services, il est nécessaire que ce processus donne des **garanties** en termes **de sécurité**. Dans cette optique, le Conseil fédéral avait annoncé être favorable à l'idée de créer un service de test d'ampleur nationale. En vue de concrétiser ce projet, l'Institut national de test pour la cybersécurité (NTC) a été créé en novembre 2020 avec le soutien financier du canton de Zoug et l'assistance technique du centre national de cybersécurité de la Confédération. Cependant, pour répondre à la demande nationale, l'Institut aurait besoin de plus de fonds. Pour ce faire, la motion de Franz Grüter (udc, LU), vice-président du NTC, aimerait intégrer la Confédération dans le financement du projet. En effet, de par les coûts financiers que l'entretien de l'Institut représente, l'attrait du secteur privé pour un tel domaine reste faible. En s'engageant financièrement, la Confédération permettrait de surmonter l'obstacle pécuniaire dans la phase d'agrandissement de l'Institut.
En se basant sur une comparaison avec l'Allemagne, le Conseil fédéral a argumenté que le secteur privé de l'informatique s'est largement développé ces dernières années. C'est pourquoi il ne serait pas nécessaire de financer directement les entreprises qui fournissent des services de tests de technologies. En effet, les entreprises devraient être capables de gérer leurs difficultés entre elles sans que l'État ne les subventionne. Ainsi, le Conseil fédéral se positionne contre cette motion.
Au Conseil national, la motion a toutefois convaincu une large majorité des députés. Le texte a été accepté par 153 voix contre 32 et 5 abstentions. [10]

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. [11]

MOTION
DATUM: 14.12.2022
CHLOÉ MAGNIN

Le passage au Conseil des États de la **motion** de Franz Grüter (udc, LU) a suscité de vives discussions. Tout a commencé dans la CPS-CE, où aucune majorité n'a été obtenue (5 voix contre 5). Le président a tranché pour l'adoption de la motion, mais les oppositions étaient importantes. Par la suite, les débats ont continué en chambre, où les député.e.s se sont demandés s'ils devaient, ou non, soutenir la formation d'un institut national de test pour la cybersécurité. En particulier, Olivier Français (plr, VD) a fait remarquer que des entreprises du secteur privé se sont lancées des défis similaires à celui du centre de cybersécurité zougois. Si elles ne semblent pas aussi avancées dans leur développement que le projet du canton de Zoug, elles auraient néanmoins du potentiel selon le sénateur. De ce fait, il ne serait pas nécessaire de subventionner et de reconnaître juridiquement cette «start-up» en développement, plutôt que d'autres entreprises. Il a aussi souhaité rappeler, en citant le Conseil fédéral, qu'«un soutien financier de la Confédération au **NTC** irait à l'encontre du principe de l'égalité de traitement et de la neutralité concurrentielle de l'État».
Dans son intervention, le conseiller fédéral Ueli Maurer a quant à lui invité à ne pas accepter la motion non seulement pour les raisons nommées dans le débat, mais aussi car l'État soutient déjà la cybersécurité par différents biais (commandement cyber de l'armée ou encore projets de recherches dans les EPF). D'après lui, ce que demande la motion ne serait donc pas nécessaire.
Bien que les acteurs principaux s'accordent sur l'importance de la cybersécurité, les arguments des opposants de la motion ont su convaincre la majorité de la Chambre des États. Ainsi, la motion a été **rejetée** par 22 voix contre 17. [12]

POSTULAT
DATUM: 16.12.2022
CHLOÉ MAGNIN

Marcel Dobler (plr, SG) a déposé un postulat au Conseil national demandant une vision globale de la stratégie des tests cyber au DDPS. Ce postulat se focalise sur les exercices de sécurité cyber et s'inscrit dans la lignée des interventions qui demandent une vue d'ensemble sur les éléments cyber et plus de collaboration entre les divers acteurs en Suisse. Pour être précis, la proposition du député Dobler consiste à élaborer et à appliquer une **stratégie globale et complète de cybertests au DDPS** pour les sept prochaines années. Cette stratégie comportera notamment des informations complémentaires concernant les exercices entrepris pour augmenter la résilience de la Suisse contre les cyberrisques. Il est aussi question de renforcer la coopération et d'acquérir de nouvelles connaissances techniques. Le député estime qu'en raison de la constante évolution du secteur cyber, le fil rouge reliant les exercices entre eux n'est pas connu. Au final, la stratégie devra répondre à «qui fait quoi, quand, avec qui et avec quels objectifs».
Le postulat a été accepté tacitement par le Conseil national, laissant une première victoire pour Marcel Dobler qui avait déjà déposé une motion traitant des mêmes problématiques, à laquelle le Conseil fédéral avait répondu négativement. La motion avait été retirée le 21 septembre 2022, soit huit jours avant le lancement de ce postulat. [13]

PARLAMENTARISCHE INITIATIVE
DATUM: 13.01.2023
CHLOÉ MAGNIN

L'**initiative parlementaire demandant la «création d'une infrastructure numérique souveraine» n'aura pas de suite**. Après les communications médiatiques d'août 2022, l'initiative a été retirée au début de l'année 2023. [14]

BUNDESRATSGESCHÄFT
DATUM: 16.03.2023
CHLOÉ MAGNIN

La CPS-CN est favorable par 16 voix contre 1 et 6 abstentions au projet qui vise à **rendre le signalement des cyberattaques envers les infrastructures critiques obligatoires**. Elle salue notamment la définition des tâches du NCSC dans la loi. La commission, considérant le sujet comme très important, a souhaité approfondir les réglementations en adoptant une proposition supplémentaire qui vise « à étendre l'obligation de signaler aux vulnérabilités des systèmes informatiques, et non seulement aux cyberattaques ».
Du côté du **Conseil national**, la sécurité numérique est considérée comme très importante par les député.e.s, ce qui s'est largement ressenti dans les discussions. Il est intéressant de relever que la minorité opposée au projet n'a pas remis en cause le but de la mesure mais les moyens employés pour y arriver. En effet, l'UDC a critiqué le choix du Conseil fédéral de punir financièrement les institutions ne reportant pas les infractions plutôt que de trouver une incitation qui motiverait tous les acteurs.
Le Conseil national a accepté l'objet par 132 voix contre 55, dont 54 provenant de l'UDC (aucune abstention). [15]

BUNDESRATSGESCHÄFT
DATUM: 21.03.2023
CHLOÉ MAGNIN

La **CPS-CE** a proposé à l'unanimité d'accepter la modification de la loi fédérale sur la sécurité de l'information (LSI) qui vise à **rendre le signalement des cyberattaques envers les infrastructures critiques obligatoires**.
Une proposition de revenir à la version initiale, avancée par le Conseil fédéral, a été évoquée. Il a en effet été suggéré de revoir la décision du Conseil national « d'obliger la signalisation des vulnérabilités concernant des moyens informatiques essentiels pour l'exploitation et encore inconnus du public ». Cette suggestion a été évincée malgré une commission très partagée. Alors que la majorité a estimé que l'effort à fournir était minime comparé aux bienfaits de la mesure, la minorité a souligné le manque d'informations vis-à-vis du nombre d'acteurs concernés et s'est montrée réticente face à une telle disposition.
La modification de la LSI sera discutée au Conseil des Etats. [16]

BUNDESRATSGESCHÄFT
DATUM: 01.06.2023
CHLOÉ MAGNIN

Le **Conseil des Etats** s'est penché sur l'objet du Conseil fédéral rendant obligatoire le **signalement des cyberattaques envers les infrastructures critiques**. Il a considéré par 31 voix contre 13 que l'obligation ne devait pas être étendue aux vulnérabilités des systèmes informatiques, comme souhaité par le Conseil national et la CPS-CE. En effet, il estime que la proposition est imprécise et que la charge administrative serait trop importante. De ce fait, la chambre haute propose de revenir à la proposition initiale du Conseil fédéral. Cette dernière a finalement été acceptée à l'unanimité. En s'opposant non seulement à sa commission mais surtout à l'autre chambre du Parlement fédéral, le Conseil des Etats renvoie l'objet au Conseil national, lançant une procédure

d'élimination des divergences. [17]

BUNDESRATSGESCHÄFT
DATUM: 20.06.2023
CHLOÉ MAGNIN

Dans le cadre de la **procédure d'élimination des divergences**, la **CPS-CN** campe sur sa position par 14 voix contre 9 et une abstention. Ainsi, elle maintient que **signaler** les **cyberattaques**, tout comme les vulnérabilités inconnues du public concernant des équipements informatiques essentiels, est crucial. Elle a cependant avancé, qu'à titre de compromis, les vulnérabilités résultant de développements internes à l'entreprise concernée pouvaient être exclues de cette mesure. En somme, seules les vulnérabilités encore inconnues du public qui pourraient nuire à une autre infrastructure critique seront annoncées. [18]

BUNDESRATSGESCHÄFT
DATUM: 11.09.2023
CHLOÉ MAGNIN

Le **Conseil national** a pris à nouveau position sur les **signalements de cyberattaques** dans le cadre de la **procédure d'élimination des divergences**. Le compromis trouvé par la CPS-CN a été soutenu par 102 voix contre 80 (aucune abstention). Le groupe UDC et le PLR se sont opposés à cette proposition, s'alignant sur la position du Conseil fédéral. Ils ont affirmé avoir conscience du défi qu'incarnent les cyberattaques, mais considèrent que rendre obligatoire la déclaration de vulnérabilités représenterait une charge administrative trop importante pour les entreprises. Le Conseil fédéral estime aussi que la confiance entre l'Etat et l'économie pourrait être renforcée, si les annonces restaient facultatives. De plus, l'UDC a souligné craindre des fuites de données qui pourraient rendre les institutions encore plus vulnérables.
Comme une majorité a été trouvée à la chambre du peuple, l'avenir de l'objet est désormais entre les mains du Conseil des Etats. [19]

BUNDESRATSGESCHÄFT
DATUM: 19.09.2023
CHLOÉ MAGNIN

Lors du premier tour de la **procédure d'élimination des divergences** , la CPS-CE est majoritairement restée campée sur la version originale du texte, celle du Conseil fédéral. Une minorité a toutefois soutenu la proposition du Conseil national, avançant une priorité: prévenir les cyberattaques. Charles Juillard (centre, JU) et Mathias Zopfi (vert-e-s, GL) l'ont résumé ainsi : «les vulnérabilités d'aujourd'hui sont les cyberattaques de demain». La minorité du **Conseil des Etats** a aussi ajouté une clause à la proposition du Conseil national, souhaitant rallonger le temps à disposition pour annoncer une vulnérabilité, passant de 24 heures à 7 jours, et souligné la possibilité d'annoncer une vulnérabilité anonymement.
Le Conseil fédéral a suivi la majorité de la CPS-CE, arguant qu'avant d'obliger les signalements des vulnérabilités, ces derniers doivent se faire sur une base volontaire, étant donné que la collaboration entre l'économie et la NCSC n'est que récente sur ce sujet. Procéder de la sorte permettrait notamment d'établir une relation de confiance entre les deux acteurs.
Le Conseil des Etats s'est alignée sur le Conseil fédéral et la majorité de sa commission, par 32 voix contre 12 (0 abstention). Selon les débats, la minorité de la chambre des cantons était principalement colorée de rose et de vert. La balle est maintenant dans le camp du Conseil national pour un deuxième tour d'élimination des divergences. [20]

BUNDESRATSGESCHÄFT
DATUM: 21.09.2023
CHLOÉ MAGNIN

Lors du **deuxième tour** de la procédure d'**élimination des divergences**, le Conseil national a revu sa position sur l'objet du Conseil fédéral qui traite du **signalement des cyberattaques**. En effet, la majorité s'est alignée sur la chambre des cantons. Ainsi, seules les cyberattaques seront annoncées, sans prendre en compte les vulnérabilités des infrastructures critiques, comme premièrement annoncé et soutenu par le Conseil fédéral. Le projet initial a été accepté par 98 voix contre 59 et une abstention.
Une semaine plus tard, le Conseil national a procédé au vote final de l'objet. Ce dernier a été accepté par 141 voix par 54 et une abstention. Seule l'UDC s'est opposée à l'objet. [21]

BUNDESRATSGESCHÄFT
DATUM: 29.09.2023
CHLOÉ MAGNIN

Suite à la proposition du Conseil national lors de la deuxième série d'élimination des divergences, le **Conseil des Etats** a clos le dossier avec un **vote final** explicite. 43 politicien.ne.s (contre 0 et 1 abstention) ont accepté que le **signalement des cyberattaques** devienne obligatoire, mais pas celui des vulnérabilités des infrastructures critiques et des systèmes informatiques. [22]

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. [23]

MOTION
DATUM: 15.03.2011
MAXIMILIAN SCHUBIGER

Anfang Juni 2010 hatte der Ständerat ein Postulat Recordon (gp, VD) (Po. 10.3136) überwiesen, welches den Bundesrat beauftragt einen Bericht zu erarbeiten, wie er dem Cyberwar zu begegnen gedenke. Ende Juni desselben Jahres wurde von der SiK-NR unter dem Titel **Massnahmen gegen Cyberwar** eine Motion mit ähnlichem Inhalt eingereicht. Diese beauftragt den Bundesrat mit der Erarbeitung gesetzlicher Grundlagen für Massnahmen zur Sicherung und Verteidigung von Datennetzwerken, die für die Schweiz und für schweizerische Einrichtungen von Bedeutung sind. Vom Nationalrat wurde die Motion in der Wintersession 2010 überwiesen. Nachdem auch der Bundesrat Anfang 2011 die Annahme der Motion beantragte, folgte der Ständerat mit dem gleichen Votum im März 2011. [24]

STUDIEN / STATISTIKEN
DATUM: 01.01.2014
MAXIMILIAN SCHUBIGER

Auch Anfang 2014 publizierte die ETH Zürich ihre gemeinsam mit dem Center for Security Studies (CSS) jährlich erstellte **Jahresstudie „Sicherheit"** zur Ermittlung der Meinungen in den Bereichen Aussen-, Sicherheits- und Verteidigungspolitik in der Schweiz. Augenfällig ist laut der Autoren eine markant positivere Einstellung der Schweizerinnen und Schweizer gegenüber der Armee. 80% der Befragten bejahen die Notwendigkeit der Armee, was einen Anstieg von 8 Prozentpunkten gegenüber 2013 bedeutet. Leicht verlagert hat sich hingegen die Einschätzung der Wehrpflicht. Gegenüber dem Vorjahr sprechen sich 37% für eine Abschaffung der Wehrpflicht zugunsten einer Freiwilligenarmee aus (+ 4 Prozentpunkte), 61% sind dagegen (eine Abnahme um 4 Prozentpunkte). Das Niveau von 2012 (48%) blieb jedoch noch immer weit unterschritten. Auch im Nachgang an die Wehrpflichtabstimmung blieb diese Haltung also gefestigt. Das bevorzugte Wehrmodell bleibt die Milizarmee, welche von einer Mehrheit von 61% (+ 5 Prozentpunkte) unterstützt wird. Einer Abschaffung der Armee stimmten im Berichtsjahr bloss noch 11% der Befragten zu (- 6 Prozentpunkte). Hinsichtlich der anstehenden Weiterentwicklung der Armee (WEA) ist interessant, wie sich die Befragten zu den Armeeausgaben äussern: 2014 hielten 49% die Kosten für angemessen, was einen Anstieg von 5 Prozentpunkten und einen Höchststand seit 1986 bedeutet. Bei der Frage nach Bedrohungsformen stehen Cyber-Angriffe an der Spitze. Auf einer Skala von 1 bis 10 wurde die Eintretenswahrscheinlichkeit eines solchen Ereignisses durchschnittlich auf 5.4 geschätzt. Einen militärischen Angriff fürchten nur gerade 3% der Befragten. Damit einhergehend sehen Schweizerinnen und Schweizer die Funktion der Armee zunehmend in subsidiären Unterstützungs- und Sicherungseinsätzen, wie der Katastrophenhilfe im Inland oder der Unterstützung der zivilen Grenzwache und der Polizei. Auf einer Zehnerskala erreicht die Armee punkto Zufriedenheit mit ihren Leistungen eine Note von 6.3. Gemessen an der langjährigen Entwicklung erreicht zudem die Beurteilung der Verteidigungsausgaben einen Höchstwert: 49% sind 2014 der Auffassung, die Höhe der Ausgaben sei angemessen. Dieser Anstieg um 5% Prozentpunkte entspricht der Abnahme der letztjährigen Einschätzung, die Ausgaben seien zu hoch. Verglichen mit dem Vorjahr, zieht sich die insgesamt positivere Einstellung der Bevölkerung gegenüber der Armee durch alle Befragungsfelder der Studie. [25]

BUNDESRATSGESCHÄFT
DATUM: 17.03.2015
MAXIMILIAN SCHUBIGER

In der Frühjahrssession hatte sich der Nationalrat mit der Vorlage zu befassen. Ohne Gegenstimme hatte die SiK beantragt, dem Entwurf des Bundesrates zuzustimmen. Die für die Periode 2016-2019 beantragten Mittel über CHF 15.4 Mio bedeuten jedoch eine Reduktion von CHF 2 Mio. pro Jahr gegenüber früheren Phasen. Kommissionssprecherin Galladé (sp, ZH) merkte an, dass damit die Erfüllung der wesentlichen Aufgaben sichergestellt werden könne. Bedenken äusserte sie namens der SiK jedoch hinsichtlich der Einsparungen im Bereich der Cyberthematik, die aufgrund der Sparmassnahmen im Konsolidierungs- und Aufgabenüberprüfungspaket auch auf diesen Rahmenkredit angewendet wurden. Verteidigungsminister Maurer brauchte nicht mehr stark für die Annahme des Kredits zu werben. Die Sorgen um eine Vernachlässigung im Bereich Cyberwar / Cyber Defense nahm er zur Kenntnis, bemerkte jedoch, dass entsprechende Anstrengungen im Gefäss einer Cyber-Strategie

unternommen werden. Das Ratsplenum beschloss Annahme des Kredits zur Weiterführung der Unterstützung des **Center for Security Studies** und Lösung der Ausgabenbremse jeweils einstimmig. [26]

MOTION
DATUM: 13.12.2017
MAXIMILIAN SCHUBIGER

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

Im Nationalrat gab es kaum eine Debatte zum Geschäft, es äusserten sich lediglich der Motionär und der Verteidigungsminister. Ersterer warb dabei erfolgreich für sein Anliegen, so dass ihm die Nationalrätinnen und Nationalräte folgten und mit 91 zu 76 Stimmen die Motion annahmen. Acht enthielten sich. [27]

MOTION
DATUM: 31.05.2018
MAXIMILIAN SCHUBIGER

Die **digitale Infrastruktur der Armee** wurde in der Sommersession 2018 mit der Motion von Claude Béglé (cvp, VD) im Ständerat zum Thema. Zwar hatte der Nationalrat zuvor den Vorstoss angenommen, die SiK des Ständerates wollte jedoch die Ablehnung der Motion durchsetzen. Eine Sistierung der Motion, um bereits in Angriff genommene Massnahmen abzuwarten, namentlich die Erarbeitung der Nationalen Strategie zum Schutz vor Cyberrisiken (NCS) und des Aktionsplans Cyberdefence (APCD), wurde diskutiert, jedoch abgelehnt. In der Kommission war man sich einig, dass im Lichte der fortgeschrittenen Digitalisierung relevante Punkte durch den Motionär angesprochen worden sind, der Vorstoss sei insgesamt jedoch zu umfangreich formuliert und ziehe womöglich nicht abschätzbare und hohe Kosten nach sich. Oben erwähnte Massnahmen würden zudem bereits zu weiten Teilen die neuen Herausforderungen durch die Digitalisierung angehen. Dies sei bereits eine adäquate Reaktion des Bundes und es sei deswegen davon abzusehen, die Motion anzunehmen.
Das Ratsplenum sah das offenbar gleich, die Motion wurde nach einer umfangreichen Berichterstattung durch Kommissionssprecher Français (fdp, VD) abgelehnt. [28]

ANDERES
DATUM: 07.11.2019
DIANE PORCELLANA

Le **Campus cyberdéfense** (CYD), fruit du partenariat entre le DDPS et l'ETH, a été inauguré. Ce partenariat fait partie du plan d'action pour la cyberdéfense et de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC). Outre la création de synergies entre l'industrie militaire, le monde académique et les communautés de hackers, la plateforme permettra d'anticiper, d'identifier et d'évaluer les tendances technologiques, commerciales et sociétales du cyberespace. [29]

PARLAMENTARISCHE INITIATIVE
DATUM: 30.09.2021
DIANE PORCELLANA

La conseillère nationale Isabelle Moret (plr, VD) demande que la Confédération se dote – en collaboration avec les cantons, le monde de la recherche et les entreprises suisses – d'une **infrastructure numérique souveraine**, notamment d'un «cloud» souverain afin de garantir une sécurisation des données sensibles et soumises au droit suisse. La Confédération se chargerait du pilotage et en supporterait les coûts.

PARLAMENTARISCHE INITIATIVE
DATUM: 19.08.2022
CHLOÉ MAGNIN

Après le passage dans les deux Commissions de l'**initiative parlementaire visant la création d'une infrastructure numérique souveraine**, une conclusion peut être tirée: cette proposition s'attaque à un problème très complexe.
Dans un premier temps, **la CPS-CN a proposé d'accepter** l'initiative d'Isabelle Moret (plr, VD) par 14 voix contre 10. Les arguments avancés par la majorité ont concerné la forme de l'accord. En effet, il est estimé par la majorité que l'État ne prendrait pas une place trop importante et que des ententes publiques-privées permettraient de renforcer la cybersécurité suisse. Cependant, une minorité de la commission ne partage pas cet avis et estime que la surveillance et la coordination qui seraient effectuées par la Confédération iraient à l'encontre du principe de la subsidiarité helvétique. Pour les opposants, il faudrait rester sur la stratégie nationale de protection de la Suisse.
Puis, dans un deuxième temps, **la CPS-CE a proposé de refuser l'initiative** par 6 voix contre 2 et une abstention. Ne remettant pas en cause le but, mais la manière, la Commission envisage de déposer une nouvelle initiative afin de revenir sur la problématique. [30]

MOTION
DATUM: 21.09.2022
CHLOÉ MAGNIN

Alors que dans l'ère du numérique les facteurs cybers jouent un rôle de plus en plus important, Marcel Dobler (plr, SG) a souhaité, en déposant une motion, mettre l'accent sur la **planification générale des exercices de sécurité** afin de consolider la résilience du système cyber suisse. Le Conseil fédéral a rejoint Dobler sur l'importance de ces exercices. C'est pourquoi ils sont inscrits sur la SNPC et que les domaines de la finance et de la santé ont déjà été sujets à ces simulations. De plus, afin de garantir une entraide et une gestion collective des complications que l'ère cyber peut engendrer, des exercices à l'échelle internationale ont déjà vu le jour. En conclusion, les objectifs de la motion ont été considérés comme atteints en raison des mesures déjà entreprises sur le territoire helvétique.
28 jours après l'annonce de l'avis négatif du Conseil fédéral, la motion a été retirée. [31]

PARLAMENTARISCHE INITIATIVE
DATUM: 11.10.2022
CHLOÉ MAGNIN

Après avoir pris connaissance de la prise de position de son homologue au conseil des États, la **CPS-CN a décidé de revenir sur sa position et propose au Conseil national de rejeter l'initiative parlementaire**. En effet, tout en soutenant le but recherché par l'écrit, la commission estime que le type de procédure n'est pas le plus adéquat. Elle doit encore réfléchir si un autre texte sera déposé. [32]

Militäreinsätze

INTERNATIONALE BEZIEHUNGEN
DATUM: 22.03.2021
DIANE PORCELLANA

La conseillère fédérale Viola Amherd a accueilli la **Ministre française des Armées**, Florence Parly, **à Berne**. Elles se sont entretenues sur différents thèmes comme la place des femmes et de l'efficacité énergétique dans l'armée, le renouvellement de la flotte aérienne et de la défense sol-air et la cyberdéfense. [33]

Militärorganisation

POSTULAT
DATUM: 16.06.2017
MAXIMILIAN SCHUBIGER

Armee 2.0 – unter dieses Schlagwort setzte Postulant Dobler (fdp, SG) die Forderungen aus seinem Vorstoss. Die Schweiz müsse das **Technologie-Know-how fördern und sichern** und entsprechend auch im Bereich der Landesverteidigung Modifikationen vornehmen, erklärte er. Fünf Punkte wurden vom St. Galler umschrieben: Das Armeepersonal müsse in Anbetracht des technologischen und wissenschaftlichen Kompetenzbedarfs rekrutiert werden; der Personalbedarf im Bereich Cyberabwehr müsse abgeklärt werden; der Bundesrat solle prüfen, inwiefern mit Bildungsinstitutionen und der Wirtschaft zusammengearbeitet werden könne; Armeeangehörigen sollten diverse neue Typen von Ausbildungen und Einsätzen angerechnet werden können; sowie, fünftens, sollten neue Kriterien der Diensttauglichkeit formuliert werden („differenzierte Tauglichkeit"). Dobler reihte sich damit in eine Gruppe von Parlamentariern ein, welche die Armee bezüglich neuerer Bedrohungsszenarien aus dem Cyberspace und durch computergestützte Systeme besser aufstellen möchte. Technologie und Wissenschaft seien immer wichtiger für die Armee und solch hoch innovativer Themen müsse sich das Militär zuwenden, so der Postulant in seiner Begründung. Einzelne Möglichkeiten zur Anrechenbarkeit von Praktika bei Bundesbetrieben oder Hochschulen an die Dienstleistung seien zwar bereits gegeben, man müsse aber noch weitere Anreize schaffen. Im Fokus stünden dabei Projekte, die für das Militär einen Verwendungszweck haben. Der Bundesrat teilte offensichtlich die Stossrichtung des Postulats und beantragte dessen Annahme. Als es im Sommer 2017 im Nationalrat behandelt wurde, gab es keine Debatte, das Geschäft wurde diskussionslos angenommen. [34]

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. [35]

BERICHT
DATUM: 11.12.2020
DIANE PORCELLANA

En exécution du postulat Dobler, le Conseil fédéral a présenté son rapport dans lequel il décrit les mesures pour **garantir les compétences de l'armée dans les nouvelles technologies**. Parmi les mesures déjà entreprises, l'accent a notamment été mis sur la formation et le perfectionnement internes, afin de faciliter l'accès des futurs spécialistes à l'administration militaire. Les militaires qualifiés dans le civil pourront être promus au rang d'officiers spécialistes ou comme spécialistes. Les spécialistes en informatique participant au stage de formation «cyber» de l'armée pourront obtenir le brevet fédéral de spécialiste en cybersécurité. Le campus cyberdéfense, la collaboration avec les partenaires suisses et étrangers, l'engagement de l'économie privée au développement des technologies liées à la sécurité, permettent de développer et conserver les connaissances technologiques. Dans le futur, le DDPS prévoit de conclure et de consolider les partenariats dans le domaine, de soutenir la recherche et le développement des technologies, ainsi que de recruter et conserver un personnel (de milice) disposant de connaissances technologiques. [36]

BERICHT
DATUM: 14.04.2021
DIANE PORCELLANA

Le Conseil fédéral soumet à consultation – jusqu'au 18 août – son nouveau **rapport sur la politique de sécurité de la Suisse**, lequel détaille les intérêts et les objectifs de la politique sécuritaire pour les années à venir. Le Conseil fédéral a décidé de procéder à des adaptations, face au contexte international en mutation et à l'apparition de nouvelles menaces. Neuf objectifs sont fixés dans le rapport: renforcer continuellement la détection précoce de menaces, de dangers et de crises; renforcer la coopération internationale, la stabilité et la sécurité; mettre davantage l'accent sur la gestion des conflits hybrides; encourager la formation libre et non biaisée de l'opinion; renforcer la protection contre les cybermenaces; enrayer le terrorisme, l'extrémisme violent, la criminalité organisée et d'autres formes de criminalité transnationale; renforcer la résilience et la sécurité de l'approvisionnement lors de crises internationales; améliorer la protection en cas de catastrophes et de situations d'urgence ainsi que la capacité de régénération et renforcer la collaboration entre les autorités et les organes de gestion des crises. Pour chacun de ces objectifs, le rapport expose les mesures spécifiques à introduire. Le précédent rapport remontant en 2016, le rapport sur la politique de sécurité sera par la suite publié une fois par législature. Le présent rapport sera soumis à l'Assemblée fédérale d'ici la fin de l'année. [37]

BUNDESRATSGESCHÄFT
DATUM: 01.09.2021
DIANE PORCELLANA

Dans le cadre de la mise en œuvre du développement de l'armée (DEVA) et en exécution de la motion 19.3427, le Conseil fédéral a soumis au Parlement une révision de la **Loi sur l'armée** (LAAM) **et l'Ordonnance sur l'organisation de l'armée** (OOrgA).
En terme d'organisation, comme décidé par l'Assemblée fédérale, la Base d'aide au commandement (BAC) et la Base logistique de l'armée (BLA) ne seront pas réunies sous le commandement du Soutien. Le Conseil fédéral propose que la BAC devienne un commandement Cyber en 2024. En matière d'instruction, les cyberspécialistes devront suivre un stage auprès de partenaires externes afin de développer leurs capacités. Dès le 1er janvier 2022, un cyber bataillon et un état-major spécialisé verront le jour, renforçant les effectifs du personnel dans le domaine de la cyberdéfense. Le Conseil fédéral demande la création d'une autorité du trafic aérien militaire, afin de davantage sécuriser les missions des Forces aériennes. Enfin, le Conseil fédéral aimerait que les recrues puissent également être engagées pour soutenir des événements civils. L'armée devrait être autorisée à fournir des prestations lors d'événements d'importance nationale ou internationale, sans forcément en tirer un avantage majeur pour l'instruction ou l'entraînement. D'autres modifications concernant notamment les droits et les devoirs des militaires doivent être faites. [38]

BUNDESRATSGESCHÄFT
DATUM: 02.11.2021
DIANE PORCELLANA

La CPS-CN propose, à l'unanimité, d'entrer en matière concernant le projet d'adaptation de la **Loi sur l'armée et l'Ordonnance sur l'organisation de l'armée** du Conseil fédéral. Les adaptations liées à la cyberdéfense ont été saluées. S'agissant de l'autorité de surveillance et de régulation du trafic aérien militaire, la commission a refusé, par 15 voix contre 10, une proposition visant à ce que les enquêtes relatives à l'aviation militaire soient menées par une commission extraparlementaire plutôt que par un service interne de l'autorité. Concernant l'appui de l'armée aux événements civils d'importance nationale ou internationale, la commission a balayé par 15 voix contre 8 et 2 abstentions, une proposition pour limiter strictement ces engagements aux cas où un bénéfice pour l'instruction était avéré. Par 17 voix contre 7, elle a rejeté une proposition visant à empêcher l'engagement de recrues. Enfin, la commission a refusé deux propositions, par 15 voix contre 9, visant à exempter du service militaire le personnel exerçant un taux d'activité d'au moins 50 pour cent et à abaisser le taux à 50 pour cent uniquement pour le personnel médical nécessaire pour assurer le fonctionnement des établissement médicaux civils. [39]

BUNDESRATSGESCHÄFT
DATUM: 15.12.2021
DIANE PORCELLANA

Avec 111 voix contre 80 et avec 179 voix et 12 abstentions, le Conseil national a approuvé **les projets de modification de la Loi fédérale sur l'armée et l'administration militaire** (LAAM) **et de l'Ordonnance de l'Assemblée fédérale sur l'organisation de l'armée** (OOrgA). La conseillère fédérale Viola Amherd a reçu le soutien de la Chambre basse pour la création d'un commandement Cyber et d'un cyber bataillon afin de renforcer la cyberdéfense. Les effectifs en la matière seront donc augmentés. Le Conseil national a également accepté la mise sur pied d'une autorité de surveillance et de régulation du traité aérien militaire, après avoir balayé par 111 voix contre 80 une proposition visant à ce que les enquêtes soient effectuées par une commission extraparlementaire. Si le PS et le PVL jugeaient qu'il serait «abusif» de mettre à disposition gratuitement des soldats sans bénéfice pour leur instruction, l'armée pourra dans le futur soutenir des événements d'importance national ou internationale sans qu'elle en retire un avantage au niveau de l'instruction et de l'entraînement. S'agissant de l'exemption de servir, la proposition visant à exempter les hommes travaillant à moins de 50 pour cent a été rejetée par 109 voix contre 80. Le personnel médical, les membres des services de sauvetage, les policiers ainsi que les gardes-frontières qui ne sont pas nécessaires aux tâches de l'armée pourront être dispensés. Pour répondre aux besoins de l'armée, le service militaire long passera de 280 à 300 jours. [40]

BUNDESRATSGESCHÄFT
DATUM: 18.03.2022
CHLOÉ MAGNIN

Le **projet de modification de l'armée et de son organisation** est passé devant le Conseil des États le premier mars 2022, après son acceptation en décembre par le national. Dans une situation militaire européenne tendue, l'ambiance a parfois été morose en ce mardi de mars sous la coupole fédérale. Les sénateurs et sénatrices ont admis dans leurs discours un besoin de se mettre à jour technologiquement afin de garantir la sécurité du pays. En décidant de suivre la position de la conseillère fédérale Viola Amherd, qui scandait la nécessité de renouveau pour faire face à des cyberattaques, les parlementaires ont approuvé le projet du Conseil fédéral. D'ici 2024, le gouvernement devra ainsi mettre en place la transformation de sa base d'aide au commandement en commandement cyber et augmenter ses effectifs dans le domaine pour passer de 206 à 575 militaires en fonction.
En ce qui concerne le deuxième point discuté, à savoir l'exemption de servir, une plus grande disparité qu'au Conseil national s'est faite ressentir. Il a été décidé que «les personnes travaillant au minimum à 80 pour cent dans le domaine de la santé, pour les services de sauvetage, dans la police, les sapeurs-pompiers et le corps des gardes-frontières, et qui ne sont pas nécessaires aux tâches de l'armée» pourront profiter de cette mesure. Concernant la demande de la gauche – que le personnel médical travaillant dans des institutions publiques à mi-temps puisse aussi profiter de cette mesure, afin de lutter contre le manque de personnel soignant –, la ministre de la défense s'y est opposée. La raison de ce désaccord est relatif au manque d'efficacité que ceci représenterait non seulement pour l'armée mais aussi pour les services de santé publique, si l'armée, exempte de ce personnel professionnel, venait à remplir sa mission de soutien au service de la santé de la population suisse. La requête est de ce fait inenvisageable pour le gouvernement helvétique.
Le projet comprenait aussi la mise en place de mesures afin de renforcer la surveillance et la participation aux manifestations des services de l'armée. De ce fait, une autorité de surveillance et de régulation de l'espace aérien militaire visant à prévenir les accidents sera créée et les militaires suisses seront plus souvent amenés à participer à des événements civils.

La modification de la loi fédérale sur l'armée et l'administration militaire (LAAM) a été acceptée à l'unanimité.
L'ordonnance de l'Assemblée fédérale sur l'organisation de l'armée (OOrgA) a, elle aussi, été acceptée à l'unanimité. Le 18 mars 2022, les deux chambres ont adopté le texte de loi final. [41]

POSTULAT
DATUM: 21.03.2022
CHLOÉ MAGNIN

Alors que la cybersécurité est actuellement l'un des sujets centraux en termes de défense nationale, la CPS-CN a déposé un postulat chargeant le Conseil fédéral d'examiner dans quelle mesure la **subsidiarité de la cybersécurité** et la **collaboration entre les différents acteurs de la cyberspace** sont envisagées au sein du DDPS.
En effet, la commission estime que la cyberspace représente un danger pour le pays et qu'une récolte d'informations est nécessaire pour minimiser les risques. Elle aimerait trouver une solution pour favoriser la coopération entre les acteurs civils et militaires afin d'augmenter l'efficacité de chacun et de lutter de manière plus optimale contre les menaces infraguerrières (par exemple: bombes, prises d'otages) qui mettent fortement en péril la sécurité de la population actuellement.
Le Conseil national et le Conseil fédéral ont soutenu le postulat. Cette décision mènera à une analyse au sein du DDPS afin de viser une meilleure compréhension de la situation actuelle et dans le but d'aboutir à de meilleures propositions d'actions. [42]

BERICHT
DATUM: 07.06.2022
CHLOÉ MAGNIN

Estimant que le postulat avait rempli son devoir, les politiciennes et politiciens fédéraux ont accepté son **classement** le 7 juin 2022. [43]

BERICHT
DATUM: 07.06.2022
CHLOÉ MAGNIN

Après la publication du rapport traitant des deux motions 19.3135 et 19.3136 nommé **«Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense»**, le Conseil fédéral a décrété que les objets devaient être classés. Ceci a été entrepris et finalisé le 7 juin 2022 dans le cadre de l'objet 22.006. [44]

Bevölkerungsschutz

ANDERES
DATUM: 20.03.2014
MAXIMILIAN SCHUBIGER

Am 20. März 2014 fand die **zweite Cyber-Landsgemeinde** des Sicherheitsverbundes Schweiz (SVS) in Bern statt. Ziel dieses Treffens von rund 70 Vertretern von Bund und Kantonen war es, über den aktuellen Stand der Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) zu informieren. Seit Ende 2013 befassen sich vier paritätisch zusammengesetzte Arbeitsgruppen mit der Umsetzung einzelner Massnahmen der Strategie in den Kantonen. Ziel dieser Massnahmen ist es, mittels konkreter Produkte die Kantone zu unterstützen, ihre Widerstandsfähigkeit zu erhöhen und Cyber-Risiken zu reduzieren. Drei Arbeitsgruppen erarbeiten in den Bereichen Risikoanalyse und Präventionsmassnahmen, Incident Management und Krisenmanagement Konzepte, Prozesse und fördern den Zugang zu Expertenwissen. Die vierte Arbeitsgruppe dokumentiert Straffälle und erstellt ein Konzept zur Koordination von interkantonalen Fallkomplexen. Der Sicherheitsverbund Schweiz koordiniert in Zusammenarbeit mit der Koordinationsstelle NCS, die beim Informatiksteuerungsorgan des Bundes angesiedelt ist, die Umsetzung der Strategie auf Stufe der Kantone und der Gemeinden. [45]

ANDERES
DATUM: 30.04.2014
MAXIMILIAN SCHUBIGER

Per Ende April 2014 lag der **Jahresbericht 2013 des Steuerungsausschusses der nationalen Strategie zum Schutz vor Cyber-Risiken** (NCS) vor. Bei vielen der 16 gefassten Massnahmen, vor allem in den Bereichen Prävention und Reaktion, wurden Ende 2013 bereits erste Meilensteine erreicht. So wurden die notwendigen Schritte zur Erstellung eines Lagebildes, das über die Cyber-Bedrohungen Auskunft geben wird, eingeleitet. In den beteiligten Verwaltungseinheiten beim Bund wurden auch nötige, neue Organisationsstrukturen geschaffen, um Cyber-Bedrohungen rasch erkennen zu können und die Handlungsfähigkeit zu erhöhen. Es wurden Grundlagen für die Zusammenarbeit geschaffen sowie einheitliche Methoden unter den beteiligten Stellen etabliert, damit im Falle von Cyber-Angriffen optimal reagiert und Schäden und Auswirkungen möglichst gering gehalten werden können.
Im Rahmen der Mitte 2012 gestarteten NCS verfolgt der Bundesrat drei strategische Ziele: die frühzeitige Erkennung der Bedrohungen und Gefahren im Cyber-Bereich, die

Erhöhung der Widerstandsfähigkeit von kritischen Infrastrukturen sowie eine wirksame Reduktion von Cyber-Risiken. Die Koordination der Umsetzungsarbeiten übernahm die bei der Melde- und Analysestelle Informationssicherung (MELANI) angesiedelte Koordinationsstelle NCS. Dort werden die Umsetzungsarbeiten überwacht und für den Einbezug aller Beteiligten gesorgt. Zusammen mit den verantwortlichen Bundesämtern wurden die Meilensteine und der Zeitplan für die jeweiligen Massnahmen definiert und in einer Roadmap festgehalten. [46]

---

1) BO CN, 2019, p.1324
2) Analyse APS des journaux 2019 – Armée
3) Communiqué de presse du DDPS du 11.12.20
4) Rapport du CF du 24.11.21
5) BO CN, 2022, p. 264 ss.; BO CN, 2022, p. 268 ss.; FF, 2021, 2895
6) Iv.pa. 21.507; Exp, 5.4.22; 24H, 6.4.22; NZZ, 30.4.22
7) BO CN, 2021, p. 2711
8) BO CN, 2022, p. 264 ss.; BO CN, 2022, p. 268 ss.
9) Communiqué de presse CPS-CE du 22.2.22; Communiqué de presse CSP-CN du 19.8.22
10) BO, CN, 2022, p.1368
11) FF, 2023 84
12) BO, CE, 2022, p.1319-1322
13) BO, CN, 2022, p. 2425
14) Communiqué de Presse du 19.08.22, 2022
15) BO CN, 2023, p. 550 ss.; Communiqué de presse CPS-CN du 21.02.23
16) Communiqué de presse CPS-CE du 21.3.23
17) BO CE, 2023, p. 385 s.
18) Communique de presse CPS-CN du 20.6.23
19) BO CN, 2023, p.1477 ss.
20) BO CE, 2023, p.791 ss.
21) BO CN, 2023, p.1831 ss.
22) BO CE, 2023, p. 1025
23) BO CE, 2010, p. 550.
24) AB NR, 2010, S. 1800 ff., AB SR, 2011, S. 251 f., AB SR, 2010, S. 550.
25) lit. Szvircsev Tresch und Wenger (2014). Sicherheit 2014
26) AB NR, 2015, S. 420 f.; BBl, 2014, S. 8909 ff.
27) AB NR, 2017, S. 2143 f.
28) AB SR, 2018, S. 358 ff.; Bericht SiK-SR vom 19.3.18
29) Communiqué de presse du DDPS du 7.11.2019; AZ, 20.3.19; LT, 28.11.19; NZZ, 6.12.19
30) Communiqué de presse CPS-CE du 22.2.22; Communiqué de presse CPS-CN du 15.2.22; Communiqué de presse CSP-CN du 19.8.22
31) Mo. 22.3836 - Curia Vista
32) Communiqué de presse du 11.10.22
33) Communiqué de presse du DDPS du 22.3.21
34) AB NR, 2017, S. 1196
35) Aktionsplan Cyberdefence
36) Rapport du Conseil fédéral du 11.12.2020
37) Communiqué de presse CF du 29.4.21; Rapport du CF du 14.4.21; AZ, TA, 30.4.21
38) Communiqué de presse du CF du 1.9.21; FF, 2021, p.2198s
39) Communiqué de presse CPS-E du 2.11.21
40) BO CN, 2021, p. 2591 ss.; Communiqué de presse du CF du 24.11.21; Communiqué de presse du CF du 24.11.21 (2); CdT, Lib, 16.12.21
41) BO, CE, 2022, pp.27 s.
42) BO, CN, 2022, p.649
43) FF, 2022, 22.006, p.34
44) FF, 2022 858
45) Medienmitteilung VBS vom 20.3.14.pdf
46) Jahresbericht Steuerungsausschuss NCS 2013.pdf; Medienmitteilung VBS vom 30.4.14.pdf