année politique suisse

DOKUMENTATION · ANALYSE · DIFFUSION

Sélection d'article sur la politique suisse

processus **Loi sur la sécurité de l'information. Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques (MCF 22.073)**

Imprimer

Éditeur

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

Contributions de

Magnin, Chloé

Citations préféré

Magnin, Chloé 2025. *Sélection d'article sur la politique suisse: Loi sur la sécurité de l'information. Inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques (MCF 22.073), 2022 - 2023*. Bern: Année Politique Suisse, Institut de science politique, Université de Berne. www.anneepolitique.swiss, téléchargé le 21.06.2025.

Sommaire

Abréviations

EFD	Eidgenössisches Finanzdepartement
SiK-SR	Sicherheitspolitische Kommission des Ständerates
SiK-NR	Sicherheitspolitische Kommission des Nationalrates
EU	Europäische Union
NCSC	Nationales Zentrum für Cybersicherheit
ISG	Informationssicherheitsgesetz

DFF	Département fédéral des finances
CPS-CE	Commission de la politique de sécurité du Conseil des Etats
CPS-CN	Commission de la politique de sécurité du Conseil national
UE	Union européenne
NCSC	Centre national pour la cybersécurité
LSI	Loi fédérale sur la sécurité de l'information

Chronique générale

Armée

Armée

OBJET DU CONSEIL FÉDÉRAL
DATE: 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. [1]

OBJET DU CONSEIL FÉDÉRAL
DATE: 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). [2]

OBJET DU CONSEIL FÉDÉRAL
DATE: 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. [3]

OBJET DU CONSEIL FÉDÉRAL
DATE: 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. [4]

OBJET DU CONSEIL FÉDÉRAL
DATE: 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. [5]

OBJET DU CONSEIL FÉDÉRAL
DATE: 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. [6]

OBJET DU CONSEIL FÉDÉRAL
DATE: 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. [7]

OBJET DU CONSEIL FÉDÉRAL
DATE: 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. [8]

OBJET DU CONSEIL FÉDÉRAL
DATE: 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. [9]

---

1) FF, 2023 84
2) BO CN, 2023, p. 550 ss.; Communiqué de presse CPS-CN du 21.02.23
3) Communiqué de presse CPS-CE du 21.3.23
4) BO CE, 2023, p. 385 s.
5) Communiqué de presse CPS-CN du 20.6.23
6) BO CN, 2023, p.1477 ss.
7) BO CE, 2023, p.791 ss.
8) BO CN, 2023, p.1831 ss.
9) BO CE, 2023, p. 1025