année politique suisse

DOKUMENTATION · ANALYSE · DIFFUSION

# Sélection d'article sur la politique suisse

processus **Cyberstratégie nationale 2023**

# Imprimer

**Éditeur**

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

**Contributions de**

Lévêque, Antoine

**Citations préféré**

Lévêque, Antoine 2025. ***Sélection d'article sur la politique suisse: Cyberstratégie nationale 2023, 2023***. Bern: Année Politique Suisse, Institut de science politique, Université de Berne. www.anneepolitique.swiss, téléchargé le 08.04.2025.

# Sommaire

# Abréviations

| | |
|---|---|
| **BA** | Bundesanwaltschaft |
| **Fedpol** | Bundesamt für Polizei |
| **NCSC** | Nationales Zentrum für Cybersicherheit |

| | |
|---|---|
| **MPC** | Ministère public de la Confédération |
| **Fedpol** | Office fédéral de la police |
| **NCSC** | Centre national pour la cybersécurité |

# Chronique générale

## Armée

### Organisation militaire

**RAPPORT**
DATE: 05.04.2023
ANTOINE LÉVÊQUE

Le **Conseil fédéral** estime que puisque les cybermenaces ont gagné en importance ces dernières années, la cybersécurité doit devenir un élément central de la politique de sécurité de la Suisse. C'est la raison pour laquelle il a décidé d'élaborer une **nouvelle cyberstratégie nationale**, qui lui permet de définir le champ d'action de la Confédération, des cantons et des acteurs privés pour faire face aux cybemenaces. Il s'est basé sur les conclusions des deux premières cyberstratégies de la Confédération, celle de 2012-2017 et celle de 2018-2022, pour rédiger cette nouvelle stratégie.
Dans la première partie de ce rapport, les auteurs s'attachent à classifier et à établir la nature des différentes cybermenaces auxquelles peut être confrontée la Suisse. Ils distinguent ainsi les menaces liées aux cyberattaques, perpétrées par des acteurs étatiques (cyberespionnage, cybersabotage) ou non-étatiques (cybercriminalité), des dysfonctionnements dus à des défaillances humaines ou techniques. A cet égard, les auteurs notent que les facteurs de cybermenaces évoluent constamment, dans la mesure où le contexte dans lequel elles s'insèrent est lui-même exposé à des changements continus. Le Conseil fédéral estime ainsi que la montée des tensions géopolitiques, dans différentes régions du monde, est susceptible de favoriser l'usage des cyberattaques contre les principaux Etats producteurs d'infrastructures informatiques, ce qui pourrait mettre en cause la capacité de la Suisse à disposer de tels outils. Parmi les technologies émergentes, dont le Conseil fédéral appelle à surveiller le développement, figure notamment l'intelligence artificielle. En effet, d'après le gouvernement, son potentiel pourrait permettre de se protéger plus efficacement contre les cyberattaques, mais aussi d'en perpétrer avec davantage de facilité.
Par la suite, le Conseil fédéral présente les efforts déployés pour faire face aux cybermenaces depuis une décennie. Il affirme que cette nouvelle cyberstratégie nationale se base sur les conclusions des deux précédentes. Mais alors que les deux premiers rapports se focalisaient sur l'implantation et le développement de structures permettant de faire face aux cybermenaces qui pouvaient viser la Suisse – par exemple grâce à la création du Centre national de la cybersécurité (NCSC) –, la présente cyberstratégie vise d'abord à définir les priorités de la Confédération en ce qui concerne les projets qui sont déjà en cours d'élaboration ou ceux qui sont envisagés pour les années à venir.
Le Conseil fédéral insiste sur le caractère multisectoriel de la politique de sécurité en vigueur en Suisse et rappelle que, puisque la Suisse est un Etat fédéral, les cantons et les collectivités territoriales disposent d'une large marge de manoeuvre dans l'application de la cyberstratégie nationale, au même titre que les acteurs privés ou les hautes écoles. Le Conseil fédéral identifie toutefois trois grands domaines d'action dans lesquels la Confédération doit jouer un rôle prépondérant : la cybersécurité, la cyberdéfense et la poursuite pénale contre la cybercriminalité. La cybersécurité, correspond à la lutte des autorités contre les cybermenaces qui visent le pays, la cyberdéfense consiste à protéger les infrastructures critiques de la Confédération contre les cyberattaques et la poursuite pénale contre la cybercriminalité ressortit aux dispositifs déployés par la Confédération et les cantons pour lutter contre la cybercriminalité. A cet égard, le Conseil fédéral précise que «la poursuite pénale pour la cybercriminalité est d'abord du ressort des cantons». Lorsque la Confédération joue un rôle en matière de lutte contre la cybercriminalité, les principaux acteurs de l'action des autorités fédérales sont l'Office fédéral de la police (Fedpol) et le Ministère public de la Confédération (MPC).
Dans ce rapport, le gouvernement s'attache également à définir les rôles qui incombent aux différents acteurs impliqués dans la nouvelle cyberstratégie nationale. Ainsi, pour renforcer les moyens d'action des cantons dans leur lutte contre la cybersécurité, il leur conseille de nommer une personne responsable de planifier leur politique en matière de cybersécurité. Par ailleurs, le Conseil fédéral a décidé de constituer un comité chargé de coordonner l'action de tous les acteurs associés à la cyberstratégie nationale. Cette démarche vise notamment à mesurer l'évolution des travaux et des projets menés dans le cadre de la cyberstratégie nationale. Le NCSC, qui assure le secrétariat de cette instance, est chargé d'informer régulièrement le Conseil fédéral de l'état d'avancement du processus de mise en oeuvre de la cyberstratégie nationale. D'après le gouvernement, l'Etat doit uniquement jouer un rôle «subsidiaire» et «partenarial» dans le déploiement de la nouvelle cyberstratégie. Cela signifie que les

institutions étatiques ne doivent intervenir que lorsque les acteurs privés ne sont pas en mesure d'agir et qu'une action de l'Etat permettrait de garantir la sécurité de l'ensemble de la collectivité.
Le Conseil fédéral identifie cinq objectifs stratégiques en ce qui concerne la lutte contre les cybermenaces. Il s'agit tout d'abord de défendre une approche qui fait la part belle à la responsabilisation des acteurs susceptibles d'être visés par des cybermenaces, notamment en intensifiant la prévention et en établissant des dispositifs permettant de mieux informer la population. Puis, le Conseil fédéral entend renforcer la fiabilité des infrastructures critiques présentes sur le territoire suisse en travaillant en partenariat avec les cantons. Le troisième objectif fixé par la Confédération relève des ressources dont disposent les autorités pour détecter, puis répondre à d'éventuels cyberincidents. En outre, le Conseil fédéral a également à coeur, comme mentionné plus haut, d'améliorer la capacité de la Confédération à engager des poursuites pénales contre les auteurs de cyberattaques. Enfin, le dernier objectif du gouvernement concernant la lutte contre la cybercriminalité, vise à permettre à la Suisse de jouer un rôle clé dans la coopération internationale contre les cybermenaces, notamment en considérant la Genève internationale comme une scène majeure des débats autour de la cybersécurité.
Dans l'ensemble, la nouvelle cyberstratégie nationale du Conseil fédéral s'attache à défendre ce qu'il appelle une «approche exhaustive basée sur les risques». Il s'agit de prendre en compte un large éventail de menaces potentielles afin de limiter au maximum les risques résiduels. [1]

1) Rapport Cyberstratégie nationale 2023