

Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2018)
Heft: [2]: Numéro Thématique 2

Artikel: Une norme pour régler un problème hors norme?
Autor: Koch, Stéphane
DOI: <https://doi.org/10.5169/seals-823450>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 14.04.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>



Le bâtiment du Ministère public de la Confédération (MPC), à Berne.

Cyber

Une norme pour régler un problème hors norme ?

Stéphane Koch

Digital strategist & digital literacy coach

L'Office fédéral pour l'approvisionnement économique du pays (OFAE) a publié un ensemble de recommandations, sous la dénomination suivante: norme minimale pour améliorer la résilience informatique. Il s'agit d'une recommandation, voire d'une ligne directrice pour améliorer la résilience informatique. Elle s'adresse en premier lieu aux exploitants d'infrastructures critiques, mais toute entreprise peut appliquer ces conseils gratuits.

La norme comprend trois parties :

- Principes de base ou guide de référence fournissant des informations sur la résilience des TIC.
- Le cadre (Framework) propose aux utilisateurs une série de mesures concrètes à mettre en œuvre. Il est subdivisé en cinq thèmes : identifier, protéger, détecter, réagir et récupérer.
- L'outil d'appréciation permet aux entreprises d'évaluer le degré de leur résilience informatique, ou de le faire vérifier par des externes (audit).

Dans la présentation de son document, l'OFAE indique : *« Il incombe à chaque entreprise d'assumer sa protection en la matière. Toutefois, comme à chaque fois qu'il en va du bon fonctionnement des infrastructures critiques, il existe une responsabilité étatique, fondée sur un mandat ancré dans la Constitution fédérale et dans la loi sur l'approvisionnement du pays. La présente norme minimale pour les TIC traduit la responsabilité de l'État qui doit protéger ses citoyens, le secteur privé, les institutions et l'administration publique. »*

Ce document est apparu le même jour où le Ministère public de la Confédération (MPC) a annoncé qu'il suspendait la procédure pénale en lien avec l'enquête visant à identifier les auteurs et/ou commanditaires des cyberattaques dont RUAG avait été victime, entre 2015 et 2016. Cette décision et ses conséquences ne sont pas

anodines. Ce n'est ni plus ni moins qu'un aveu public d'échec. Et c'est aussi la troisième fois que le MPC classe un cas de ce type. Les départements des Affaires étrangères et de la Défense, avaient également subi des cyberattaques en 2017.

C'est un message inquiétant qui a été envoyé à tous ceux qui pourraient viser les intérêts de la Suisse. Que cela soit au niveau économique, politique, ou stratégique. Ce type de cyberattaques pourrait être considéré comme une version moderne et dématérialisée d'une stratégie asymétrique. La nouvelle (cyber) arme de la géopolitique et de la guerre économique.

A la différence que ce n'est pas nécessairement le faible qui attaque le fort, du moins si on réfléchit en termes de capacité à se défendre par celui qui est attaqué. Dans cette nouvelle dynamique, le fort peut aussi être le faible. La Suisse est forte économiquement, mais faible dans sa capacité à se défendre, ce qui en fait une cible d'autant plus intéressante. Et l'annonce du MPC sonne comme une confirmation de cette situation de faiblesse.

Il est véritablement temps qu'une prise de conscience s'opère de manière transversale, d'abandonner le fédéralisme de la gouvernance, comme celui des idées, afin de faire fi des dissensions et laisser enfin la place à une stratégie unie et concertée, à même d'anticiper et au besoin, d'avoir la capacité d'endiguer ou de stopper des attaques cybernétiques dont notre pays est l'objet.

Il ne s'agit pas de uniquement de protéger les infrastructures critiques de notre pays, mais de comprendre que la sécurité de ces infrastructures, entre autres, protège l'économie et la souveraineté de la Suisse.

Pour y arriver, il s'agit aussi de réussir à protéger les entreprises et les particuliers, des risques cyber. Il faut

