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

Vorwort: Les cyber défis
Autor: Vautravers, Alexandre

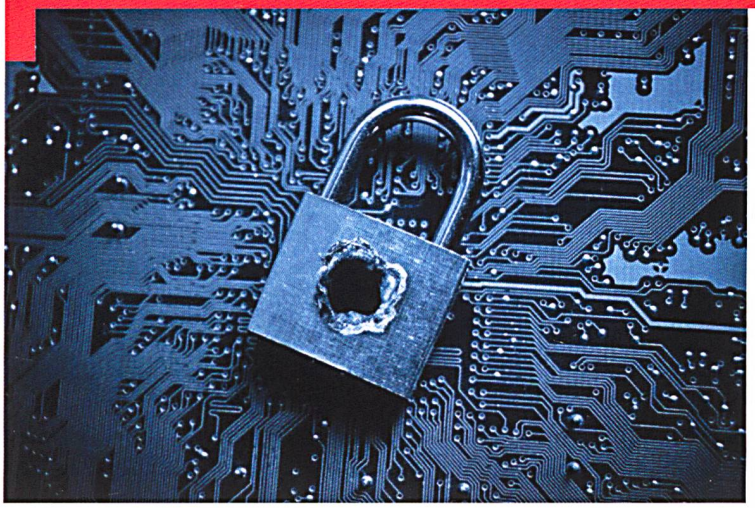
Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. 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: 07.01.2026

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



La sécurité des données et des réseaux informatiques, ainsi que l'efficacité du droit, sont des facteurs essentiels de la résilience ainsi que de l'attractivité de l'économie suisse.

Edito

Les cyber défis

Col EMG Alexandre Vautravers
Rédacteur en chef, RMS+

Contrairement au domaine de la défense terrestre ou même aérienne, qui connaissent des frontières visibles, reconnues internationalement, le domaine des télécommunications électromagnétiques, des réseaux informatiques, du stockage des données, des serveurs ou des prestataires de service en ligne pose des questions stratégiques d'un nouvel ordre.

L'environnement numérique des technologies de l'information et de la télécommunication (TIC) est basé sur des infrastructures et des réseaux largement ouverts, interconnectés et transnationaux, à la manière d'un échiquier ou d'un réseau d'autoroutes. Il existe aussi beaucoup de nœuds et de carrefours, alors qu'il n'existe en contrepartie que très peu de passages obligés, du moins en Europe.

Pas de grande muraille

Il n'y a pas de « muraille » ou de défense « linéaire » efficace. Celles-ci, généralisées sur un tel réseau, sont de coûteuses illusions. Il n'est pas non plus possible de confier à un seul acteur ou à une seule agence le rôle de policier sur ce réseau si vaste, en croissance permanente et largement internationalisé.

Comme au Moyen-Age, les fortifications des villes ou des bourgs ont remplacé le *limes romain*. Il faut désormais que chacun prenne ses responsabilités et soit en mesure d'assurer sa protection, autonome, jusqu'à l'arrivée des secours.

Centre et périphérie

Prenons cependant garde aux images. Car contrairement à la géographie et au domaine physique, où l'on construit des couches de protection superposées – afin de « durcir » des objectifs, le domaine cyber se joue largement des distances et des murs anti-feu. La ruse, les erreurs de manipulation, les agents infiltrés ou achetés, les fuites, les défauts de conception, les accès dérobés, la reprise de logiciels ou de codes, sont autant de vulnérabilités.

Contrairement à la théorie des cercles concentriques de John Warden, il est désormais possible de passer par des souterrains numériques, de disposer d'un effet de surprise important afin de frapper au cœur les centres de gravité de l'adversaire.

Ces images nous montrent que les défis sont considérables et coûteux. Ils nécessiteront la mise sur pied de moyens et de protocoles minimaux de sécurité généralisés: le GDPR et les nouvelles normes internationales en sont une partie. Ils s'accompagneront d'une stratégie et de moyens d'actions nationaux efficaces, au besoin d'une assistance transfrontalière nécessaire. La Confédération développe et affine depuis plusieurs années sa propre stratégie cyber.

Tactique et stratégique

On peut d'ores et déjà distinguer deux niveaux : le premier lié à la petite criminalité informatique et dont les cantons – en premier lieu la police – jouent un rôle prépondérant. Le second échelon est stratégique et touche la Confédération, ses systèmes de communication ou ses infrastructures critiques. Lorsque des attaques de large ampleur sont détectées, il devient alors nécessaire d'engager les moyens stratégiques – actuellement répartis au sein de plusieurs départements.

Quant aux entreprises, aux collectivités publiques, elles occupent en quelque sorte un échelon intermédiaire, opératif, car la porosité des barrières et des systèmes peut conduire rapidement à l'escalade ou à des effets de cascade, d'un système à un autre.

Les défis et les acteurs sont nombreux. Les initiatives existent et doivent désormais être coordonnées, synchronisées, afin de gagner en efficacité. C'est la présentation de ce nouveau « champ de bataille », à la fois étendu et profond, que la RMS vous propose avec ce numéro thématique.

A+V