Les cyber défis

Autor(en): **Vautravers, Alexandre**

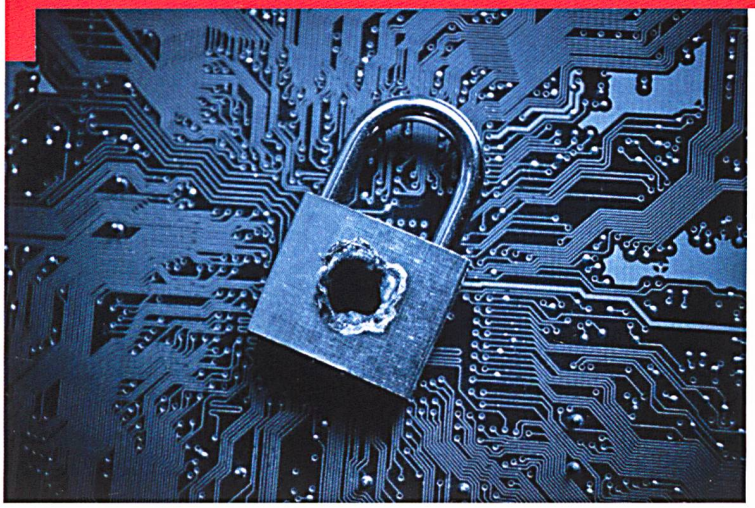
Objekttyp: **Preface**

Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2018)**

Heft [2]: **Numéro Thématique 2**

PDF erstellt am: **16.05.2024**



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