Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2008)
Heft: 2

Artikel: La cyber-défense de la Suisses
Autor: Baudoin, Guillaume
DOI: https://doi.org/10.5169/seals-346843

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: 12.07.2025

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

Les communications militaires (ici INTAFF dans un véhicule commandant de tir) ne sont pas les seules à être vulnérables et à devoir être protégées.

La cyber-défense de la Suisse

Lt Guillaume Baudoin

Cet article est paru dans *Eclairage* No.1, 2008, le Bulletin de la Société militaire de Genève.

Dans la guerre asymétrique, lorsque les moyens d'une partie sont limités par le nombre de fusils d'assaut ou de lance-roquettes disponibles, les moyens à engager pour assurer la défense sont connus. Mais lorsqu'il s'agit d'informatique, quand un petit groupe d'attaquants peut prendre le contrôle d'une armée d'agents contaminés, l'effet de surprise peut-être total. Le 27 avril 2007, une attaque a été lancée contre le réseau de communication de l'Estonie. Les transactions bancaires, qui se font à plus de 97 % en ligne[1] ont été impossibles, immobilisant ainsi toute l'économie du pays. Un pays européen à la pointe dans son infrastructure de télécommunications s'est retrouvé coupé du monde pendant plusieurs jours.

Afin de pouvoir contrer cette menace, l'OTAN va établir en Estonie un centre de compétence de cyber-défense et la marine américaine y enverra un de ses meilleurs experts[2]. Le développement du centre d'excellence se fera à partir du centre de compétence existant des Forces armées estoniennes.

La Suisse, de par sa position géographique centrale et la présence d'organisations internationales fondatrices du Web actuel, est un carrefour des autoroutes de l'information. Plus de 75 % de la population suisse utilise l'Internet[3] pour des activités diverses telles qu'effectuer des paiements bancaires, se former, ou communiquer. Plus de la moitié des entreprises y ont recours pour leurs activités régulières[4]. La démocratie de notre pays s'exerce de plus en plus via l'Internet, comme le prouve l'expérience d'*e-voting*, à Genève.

La défense de l'infrastructure Internet en Suisse est actuellement organisée avec en première ligne MELANI,[5] un service d'annonce et d'alertes et SONIA,[6] une cellule de crise mobilisable pour la sûreté de l'information. Ces services utilisent le centre de réaction aux urgences informatiques de l'organisme SWITCH, qui n'est pas opérationnel en dehors des heures de bureaux.[7]

L'Europe peut elle se permettre d'avoir en son cœur un point faible ? L'armée suisse doit-elle s'équiper, elle aussi, d'une structure capable de prévenir les attaques informatiques, de minimiser leur impact ou d'organiser une défense active ?

G.B.

1 www.whitehouse.gov/news/releases/2007/06/20070625.html
2 www.mod.gov.ee/?op=news&id=1335
3 www.bfs.admin.ch/bfs/portal/fr/index/themen/16/04/key/
4 www.bfs.admin.ch/bfs/portal/fr/index/themen/16/04/key/
5 MELANI : Melde und Analysestelle Informationssicherung : Centrale d'enregistrement et d'analyse pour la sûreté de l'information.
6 SONIA : Sonderstab Informationssicherung : Etat-major de sûreté de l'information.

7 /www.switch.ch/cert/