

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

Artikel: De la difficulté de penser l'applicabilité d'un cadre juridique aux cyberopérations étatiques déployées en temps de paix
Autor: Dabour, Ataa
DOI: <https://doi.org/10.5169/seals-823452>

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: 24.02.2026

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

Les mêmes questionnements resurgissent lors de chaque cyberaction. Comment déterminer quel acteur est responsable de quelle cyberopération, comment évaluer si celle-ci entre dans le cadre de la cyberguerre ou non, et si elle nécessite donc une réponse militaire ou non. Pour le moment, ce qui relève de la cyberguerre est « *une question de perception* », ⁵ explique Mr. James Clapper, directeur du renseignement américain. Même l'applicabilité d'un cadre juridique aux cyberopérations déployées dans le cadre de conflits armés semble dès lors être floue.

Finalement, il convient de souligner que les deux concepts de cyberguerre et de cyberpaix sont interconnectés puisqu'à mesure que l'emploi de la cyberguerre inter-étatique augmente, l'idée d'une cyberpaix se renforce. Alors, comment penser à un cadre juridique applicable aux cyberopérations menées en temps de paix sans avoir préalablement pensé et défini les concepts de cyberguerre et de cyberpaix, leurs contours ainsi que leurs implications ?

Conclusion

Lors de la 12^e rencontre annuelle du Forum sur la Gouvernance d'Internet qui s'est déroulée à Genève du 18 au 21 décembre 2017, le président de Microsoft, Brad Smith, s'était exprimé sur la nécessité de réglementer les cyberopérations en temps de paix. Grâce à cette démarche, la Convention de Genève du digital est née. Mais, celle-ci traite uniquement des cybeactions conduites au sein des entreprises, sans faire référence aux États.

La réglementation des cyberopérations étatiques déployées en temps de paix a fait l'objet de nombreuses discussions. Mais la complexité de cette question vient du fait qu'elle dépend d'autres questions sous-jacentes, auxquelles il est crucial d'apporter, de prime abord, des réponses. Il apparaît par exemple qu'il est d'abord nécessaire de définir ce qu'est une cyberguerre et la manière dont on détermine qu'une cyberattaque entre dans la catégorie de cyberconflits ou non.

Dès lors, la problématique de la cyberpaix émerge – car, après tout, l'existence d'une cyberpaix relève directement de l'absence de cyberguerre. Quelles sont donc les conditions déterminantes d'une cyberpaix ? Cette question a été pour la première fois débattue lors de la conférence internationale « Construire la paix et la sécurité internationale de la société numérique » le 6 et 7 avril 2017 au siège de l'UNESCO – avec la participation du Secrétariat général de la Défense et de la Sécurité internationale (SGDSN) et de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Pour désamorcer les débats autour de l'applicabilité d'un cadre juridique aux cyberopérations étatiques en temps de paix, ne serait-il pas devenu utile d'élargir le débat autour de la cyberpaix ?

A. D.

Suite de la page 21

Ce n'est pas parce que la lutte contre la cybercriminalité est onéreuse et complexe qu'il ne faut rien faire ou en déléguer tout ou partie des activités. Externaliser les fonctions de la lutte contre la cybercriminalité, à des acteurs privés, pour des raisons économiques et de compétence, engendre une perte de la capacité régaliennne de l'Etat, une perte d'autonomie, d'indépendance et de souveraineté.

Une bonne compréhension des enjeux géopolitiques, sociaux et économiques de l'écosystème numérique, de la cybersécurité, de la cyberdéfense et de la cyberdiplomatie est incontournable pour assurer la stabilité de la Suisse au XXI^e siècle.

S. G.

Un livre pour en savoir plus: S. Ghernaoui *La cybercriminalité, les nouvelles armes de pouvoir*. Le savoir suisse, PPUR 2017. Prix du livre Cyber du Forum International de la Cybersécurité. Lille 2018.

⁵ François, Camille, *Penser la Cyberpaix*, in Le Monde Diplomatique, Avril 2016. (<https://www.monde-diplomatique.fr/2016/04/Francois/55211#nb10>).

Intelligent Cybersecurity

Innovation. Every Day.



Conseil



Technologies



Services Managés



Recherche &
Innovation

Kudelski Security
Route de Genève 22-24
1033 Cheseaux-sur-Lausanne

Kudelski Security
Löwenstrasse 65-67
8001 Zürich

Info@kudelskisecurity.com | www.kudelskisecurity.com

 Kudelski Security |  @KudelskiSec