De la difficulté de penser l'applicabilité d'un cadre juridique aux cyberopérations étatiques déployées en temps de paix

Autor(en): **Dabour, Ataa**

Objekttyp: **Article**

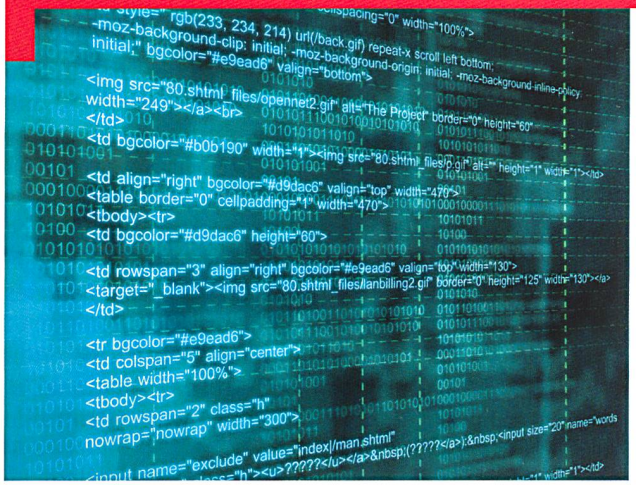
Zeitschrift: **Revue Militaire Suisse**

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

Heft [2]: **Numéro Thématique 2**

PDF erstellt am: **21.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-823452



International

De la difficulté de penser l'applicabilité d'un cadre juridique aux cyberopérations étatiques déployées en temps de paix

Ataa Dabour
Etudiante, MAS en sécurité globale et résolution des conflits, Université de Genève

Ces dernières années ont été marquées par la multiplication de cyberopérations interétatiques. On assiste en 2007 à une série de cyberattaques menées par la Russie contre les banques, les journaux et les serveurs de l'administration de l'Estonie. Une année plus tard, la Géorgie connaît à peu de chose près le même sort. En 2010, l'Iran doit faire face au virus *Stuxnet* dirigé par les Etats-Unis et Israël afin d'espionner et de reprogrammer des systèmes industriels ainsi que des centrales hydroélectriques et nucléaires.

Désormais, conscientes que tout conflit comporte une dimension numérique, les grandes puissances commencent à s'organiser. En 2008, les Etats-Unis sont les premiers à mettre en place un sous-commandement voué aux cyberopérations, le US Cybercom. Aujourd'hui, plus d'une soixantaine de pays ont/ou développent des outils de cyberespionnage et de cyberattaques.[1]

Toutefois, il y un problème: alors même qu'« *une grande part des opérations familièrement qualifiées de cyberattaques (...) ont lieu hors du cadre d'un conflit armé,* »[2] comme l'explique Cordula Ddroege, conseillère juridique au CICR, « *la guerre de l'information concerne uniquement les opérations informatiques menées en période de conflit armé et exclut toutes celles menées en temps de paix* »[3] souligne Michael Schmitt, président du département de droit international au Naval War College. De fait, la définition d'un cadre juridique applicable aux cyberactions étatiques menées en temps de paix est essentielle. Toutefois, les questionnements que soulèvent un tel travail sont toutefois complexes.

Difficultés

En 2009, un groupe d'expert est mandaté par l'OTAN pour se pencher sur le cadre juridique international applicable aux cyberopérations. La question était alors de savoir comment le droit international des conflits armés s'applique-t-il aux confrontations dans le cyberespace ? Publié en 2013, le Manuel de Tallinn en est le résultat. Ce manuel comporte quelques normes et règles qui régissent les cyberactions interétatiques en temps de guerre. Mais, rien sur celles qui ont lieu en période de paix. Le droit international humanitaire (DIH) ne peut être invoqué puisque celui-ci ne rentre en compte que si les cyberattaques se produisent dans le cadre de conflits armés - « *que ce soit entre des États, entre des États et des groupes armés organisés ou entre des groupes armés organisés.* »[4]

Plusieurs raisons peuvent expliquer pourquoi définir un cadre juridique applicable aux cyberopérations étatiques, surtout celles menées en temps de paix, est problématique. La première difficulté est l'absence de normes comportementales dans le cyberespace universellement acceptées. La seconde réside dans le fait que la notion-même de cyberguerre, ses contours et ses implications ne sont toujours pas clairement définis.

1 Valentino-DeVries Jennifer; Thuy Vo, Lam; Yadron, Danny, "Cataloging the World's Cyberforces," in *The Wall Street Journal*, 28 December 2015. (http://graphics.wsj.com/world-catalogue-cyberwar-tools/). Tous les sites ont été consultés du 3 au 7 juillet 2018.

2 Droege, Cordula, *Pas de vide juridique dans le cyberespace*, in Comité international de la Croix-Rouge, 16 Août 2011. (https://www.icrc.org/fre/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm).

3 Moreau, Cécile, *Les cybertechnologies: le droit international humanitaire a-t-il un avenir avec les cyberconflits?*, p.1-10 (http://civirdepa.e-monsite.com/medias/files/dih-et-cyberconflit-1.pdf).

4 Droege, Cordula, *Pas de vide juridique dans le cyberespace*, in Comité international de la Croix-Rouge, 16 Août 2011. (https://www.icrc.org/fre/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm).

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 12e 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.

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

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 régalienne 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 XXIe siècle.

S. G.

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

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

in Kudelski Security | @KudelskiSec