CHAIRE DE CYBERDÉFENSE ET CYBERSÉCURITÉ
SAINT-CYR THALES SOGETI

Les notions de guerre et de paix dans le cyberespace

Sarah Gorguos (Mastere, Université de Sherbrooke)

Juillet 2013, article n°III.10

La guerre et la paix sont des notions anciennes, définies par la politique internationale et le droit international. Depuis la fin du XIXème siècle, le développement des technologies de l'information a ouvert des perspectives nouvelles[1]. Au cours des années 1990 s'est accrue la prise en compte du cyberespace[2], qui est « un espace caractérisé par l'utilisation de l'électronique et du spectre électromagnétique pour vendre, échanger ou modifier des données, par le biais de systèmes informatiques et des structures physiques associées »[3]. Le cyberespace pose des problèmes inédits à la politique et au droit, puisqu'il transcende les conceptions de territoire et de frontière, rendant obsolètes les définitions de la guerre et de la paix. Or, le cyberespace est de plus en plus présent dans les stratégies de cybersécurité étatiques. La volonté politique et le comportement des États vis-à-vis de la cyberdéfense influencent grandement la manière dont la guerre et la paix sont appréhendées dans ce cadre virtuel. Le problème est donc le suivant : la guerre et la paix sont-elles des notions qui ont un sens dans le cyberespace ? Pour y répondre, il est nécessaire d'étudier en premier lieu les définitions juridiques et politiques de la guerre et de la paix, puis en second lieu, pourquoi, d'un point de vue étatique, le cyberespace est un enjeu majeur concernant les deux notions.

1 - L'inadéquation des définitions juridiques et politiques traditionnelles de la guerre et de la paix au cyberespace

Les définitions juridiques stato-centrées de la guerre et de la paix, un frein à l'application du droit international au cyberespace

Un conflit armé international existe dès lors qu'il y a « un recours à la force armée entre deux ou plusieurs États »[4], la paix étant généralement définie comme une absence de conflit. L'article 2 paragraphe 4 de la Charte des Nations Unies prohibe le recours, dans les relations entre les États Parties, « […] à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance

[1]VENTRE, Daniel. *Cyberattaque et cyberdéfense*, Paris, Lavoisier, 2011, p. 9.

[2]VENTRE, Daniel. *La guerre de l'information*, Paris, Lavoisier, 2007, p. 13.

[3]JOINT CHIEFS OF STAFF. « Joint Terminology for Cyberspace Operations », Département de la Défense, États-Unis, 2010, p. 7, traduction libre de « Domain characterized by the use of eclectronics and the electromagnetic spectrum to store, modify and exchange data via networkeesystems and associated physical infrastructures ».

[4]CICR. « Comment le terme « conflit armé » est-il défini en Droit International Humanitaire ? », 2008, p. 5.

politique de tout État [...]»[5]. Une agression armée doit être imputable à un État et se caractérise notamment par son intensité et par le fait qu'elle porte atteinte au territoire d'un État[6]. L'applicabilité du droit international des conflits armés (jus ad bellum et jus in bello[7]) dépend donc de l'imputabilité des actes aux États concernés[8], ou de l'identification du territoire sur lequel se déroulent les hostilités. La notion de frontière est prédominante[9] et l'intensité du conflit ou de l'attaque a son importance. Or, un cyberconflit se caractérise par son aspect immatériel, déterritorialisé[10] : il se situe au-delà des frontières étatiques[11], puisqu'il peut provenir, ou se dérouler sur le territoire de plusieurs États. Une cyberattaque est rapide et anonyme, donc difficilement imputable à un Etat[12]. La question de savoir si une cyberattaque constitue un emploi de la force génère d'importants débats en doctrine, n'est pas tranchée en droit et dépend de l'interprétation que l'on fait de l'article 2 paragraphe 4 de la Charte[13]. De plus, l'intensité et les dommages d'une cyberattaque sont difficilement appréciables[14]. Pour les mêmes raisons, la notion d'agression armée est également peu adaptée en cas de cyberattaque. Laisser au Conseil de sécurité le travail de qualification reviendrait à courir le risque que l'application du droit international ne soit paralysée par l'exercice du droit de veto. Ainsi, les définitions actuelles de la guerre et de la paix en droit international sont un frein à son application aux cyberconflits.

Des définitions politiques plus larges mais inadaptées à l'évolution du caractère de la guerre : la nécessité d'adapter la théorie à la pratique

En dehors du droit, la guerre peut être définie comme « […] un conflit entre des groupes politiques, notamment des États souverains, opposant des forces armées d'une ampleur considérable pendant une longue période de temps »[15]. Là encore, la paix s'entend généralement de l'absence de guerre. En matière politique, les définitions ne sont plus adaptées aux modalités nouvelles des conflits armés, tels que la cyberguerre[16]. Or, cette dernière prend de l'importance dans les stratégies militaires des États[17]. Il faut donc en cerner les caractéristiques, comme l'a souligné le Département de la Défense américain, selon lequel le vocabulaire militaire n'est pas adapté au cyberespace[18]. Certains ont défini le cyberconflit comme « […] une opération coordonnée, menée au travers du cyberespace par un groupe ayant des objectifs définis, au moyen de systèmes d'information et de communication »[19], ce qui est bien trop vague. Ce travail de définition doit tenir compte de la tension inhérente au concept de cyberguerre. La définition de la cyberguerre doit permettre de différencier les cyberattaques à caractère militaire des autres cyberattaques[20]. Cette définition doit être suffisamment restrictive pour

[5]*Charte des Nations Unies (et Statut de la Cour Internationale de Justice)*, 26 juin 1945, C.N.U.O.I.
[6]*Définition de l'agression*, Rés., Doc. off. AG, 29e sess., Doc. N.U. 3314 (14 décembre 1974).
[7]Pour une définition des deux notions, voir KASKA, Kadri ; KERT, Mari ; RÜNNIMERI, Kristel ; TALIHÄRM, Anna-Maria ; TIKK, Eneken ; VIHUM, Liis. « Cyber Attacks Against Georgia : Legal Lessons Identified », Cooperative Cyber Defense Centre of Excellence, 2008, pp. 18-19.
[8] ANDRES, Richard B. ; SHACKELFORD, Scott J. « State Responsibility for Cyber Attacks : competing Standards for a Growing Problem », *Georgetown Journal of International Law*, 2011, vol. 42, n°4, p. 971.
[9] POST, David G. « Governing Cyberspace : Law », *Santa Clara Computer and High-Technology Law Journal*, 2008, n°4, p. 885.
[10]STELLA, Marie. « La menace déterritorialisée et désétatisée : le cyberconflit », *Revue internationale et stratégique*, 2003, vol. 49, n°1, p. 167.
[11]POST, D. G., préc., note 9, p.
[12]ANDRES, R. B. ; SHACKELFORD, S. J. ; préc., note 8, p. 971.
[13]ROSCINI, Marco. « World Wide Warfare – Jus ad bellum and the use of cyber force », *Max Planck Yearbook of United Nations Law*, 2010, vol. 14, p. 105.
[14] LOUIS-SIDNEY, Barbara. « La dimension juridique du cyberespace », *Revue internationale et stratégique*, 2012, vol. 3, n° 87, p. 80.
[15]WRIGHT, Quincy., *A Study Of War*, Chicago, Chicago University Press, 1965, Cité dans SHEEHAN, Michael, « Le caractère changeant de la guerre » dans BAYLYS, John ; SMITH, Steve ; OWENS, Patricia. La globalisation de la politique mondiale -Une introduction aux relations internationales, Montréal, Modulo, 2011, p. 224.
[16]VENTRE, D., préc., note 1, p. 189.
[17]BAUD, Michel. « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », *Politique Étrangère*, 2012, n°2, p. 305.
[18]JOINT CHIEFS OF STAFF. « Joint Terminology for Cyberspace Operations », Département de la Défense, États-Unis, 2010, p. 1.
[19] BAUD, M., préc., note 17, p. 307.
[20]CENTER FOR SECURITY STUDIES. « Cyberguerre : concept, état d'avancement et limites », *Politique de sécurité : analyses du CSS*, n°71, 2010, p. 1.

que le terme de cyberconflit ne soit pas utilisé pour qualifier tous types d'agressions[21]. Mais elle doit être assez souple pour caractériser toutes les cyberguerres, qui ne répondent pas toujours aux critères habituels de la guerre[22]. Elle doit englober toutes les formes « d'opérations dans les réseaux informatiques »[23] et tenir compte de tous les aspects des cyberconflits et pas seulement de son aspect technologique[24]. Ainsi, les définitions politiques de la guerre et de la paix doivent être réadaptées, et des définitions adéquates de la cyberguerre et de la cyberpaix doivent être élaborées.

2 - Le cyberespace, un enjeu majeur pour la guerre et la paix

La cybersécurité des États, un facteur de conflits plutôt que de paix

L'examen des stratégies de cybersécurité des États-Unis[25] ou de la France[26] prouve que les États se préparent pour se protéger des cyberattaques et pour y répliquer, dans une sorte de course aux cyberarmements[27]. Toutefois, la Russie et la Chine notamment ont soutenu la création d'un Code de conduite sur internet[28]. Malgré cela, les cyberattaques dont a été victime l'Estonie en 2007 sont imputées à la Russie[29]et la Chine est pour les États-Unis l'un des plus grands dangers du cyberespace[30]. Les stratégies de cybersécurité des Etats doivent cependant opérer sur un plan défensif et offensif, pour compenser le caractère asymétrique des cyberconflits et parvenir à un équilibre entre résilience et perturbation[31]. Des limites, notamment juridiques sont nécessaires pour maîtriser les conséquences de ces stratégies. En l'absence de définitions juridiques et politiques adaptées de la guerre et de la paix, ces limites sont impossibles à tracer. De plus, tous les États ne souhaitent pas encadrer le cyberespace[32]. La cybersécurité des États peut donc être une source de conflits armés[33]. D'un point de vue constructiviste, la nature de l'anarchie qui domine le système international est déterminée par les identités, les perceptions, les intérêts et les actions des Etats[34]. Le cyberespace est un système de compétition, comme en témoignent la course aux cyberarmements et la nature masquée des cyberattaques, rarement imputables à un État, et ne constituant pas une confrontation directe. L'enjeu est donc que cette sorte de « cyberpaix armée »[35] ne dégénère pas en conflit armé ouvert.

Les obstacles politiques et juridiques au contrôle des cyberarmements

Selon le Code pénal français, une cyberarme est « un équipement, un instrument, un programme informatique [...] »[36]. Ce qui la distingue d'un programme informatique innocent est donc l'intention

[21] BAUD, M., préc., note 17, p. 306.
[22]VENTRE, D., préc., note 1, pp. 189-190.
[23] CENTER FOR SECURITY STUDIES, préc., note 20, p. 2. Détaille quelles sont les trois formes d'opérations possibles.
[24]SAMAAN, Jean-Loup. « Mythes et réalités des cyberguerres », Politique étrangère, 2008, n°4, p. 837.
[25]US DEPARTMENT OF DEFENSE. *Department of Defense Strategy for Operating in Cyberspace*, juin 2011, p. 13.
[26]AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION. « Défense et sécurité des systèmes d'information. Stratégie de la France », 2011, p. 11.
[27]VENTRE, Daniel. « La cyberpaix : un thème stratégique marginal », *Revue internationale et stratégique*, 2012, vol. 87, n°3, p. 90.
[28]MINISTRY OF FOREIGN AFFAIRS OF THE PEOPLE'S REPUBLIC OF CHINA. China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations, 2011, [en ligne].
[29]SHACKELFORD, Scott J. « From Nuclear War to Net War : analogizing Cyber Attacks in International Law », *Berkeley Journal of International Law*, 2009, vol. 57, n°1, p. 207.
[30]US-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. *2012 Annual Report to Congress*, 2012, p. 168.
[31]DEMCHACK, Chris C. « Organiser sa défense à l'ère du cyberconflit : un point de vue étatsunien », *La Revue internationale et stratégique*, 2012, n°87, p. 109.
[32]LOUIS-SIDNEY, B., préc., note 14, p. 82.
[33]VENTRE, D., préc., note 27, p. 86.
[34]WENDT, Alexander. « Anarchy is What States Make of It : The Social Construction of Power Politics », *International Organization*, 1992, vol. 46, n°2.
[35]Centre National de Ressources Textuelles et Lexicales, Définition de la paix, [en ligne], cité dans VENTRE, D., préc., note 27, p. 90.
[36]Nouveau Code pénal, art. 323-3-I.

avec laquelle elle est utilisée ou créée[37]. Comme le montre l'exemple du virus Stuxnet[38], une cyberarme n'est identifiable qu'une fois utilisée, l'intention étant une notion subjective et difficile à déterminer. Il est impossible de réglementer les cyberarmes par analogie avec le droit applicable aux armes nucléaires par exemple[39]. Cette réglementation n'est possible qu'a posteriori, une fois que la cyberarme a été utilisée et ne peut être autonome : elle dépend de l'identification d'une cyberattaque, puisque l'arme doit avoir servi dans cette intention. Le contrôle des cyberarmes se heurte donc à l'inadéquation des définitions du droit au cyberespace. Pour être qualifiée d'agression armée, la cyberattaque doit avoir causé d'importants dommages humains ou matériels[40] et être imputable à un État, éléments très difficiles à établir. De plus, l'impossibilité d'établir la responsabilité de quiconque détient de telles armes sans les utiliser, inciterait les États à s'en procurer et serait un obstacle à l'efficacité du contrôle, à cause de son caractère a posteriori. Au niveau international, le contrôle des armements classiques se heurte à la volonté politique des États, comme en témoigne l'opposition aux mécanismes de vérification du respect de la Convention sur les armes biologiques de 1975[41]. Il est fort probable que la réglementation des cyberarmes rencontre un tel problème, de manière accentuée.

Conclusion

La raison pour laquelle la cyberpaix doit être assurée permet également de conclure que les notions de guerre et de paix ont un sens dans le cyberespace. Il y a une grande perméabilité entre le réel et le virtuel. Les conflits actuels comprennent une dimension virtuelle[42]. Les cyberattaques ont des conséquences réelles, comme l'ont démontré les attaques subies par l'Estonie en 2007[43]. Il est nécessaire d'assurer la cyberpaix en raison de la grande dépendance des sociétés aux technologies de l'information[44]. Toutefois, ces dernières peuvent être un outil de reconstruction de la paix, en ce qu'elles facilitent les actions humanitaires[45]. Mais le caractère virtuel du cyberespace rend les menaces qui s'y font jour difficiles à appréhender, la perception de leur gravité est faussée. Assurer la cyberpaix nécessite un travail de définition politique et juridique, afin de cerner ce qui pourrait lui porter atteinte. Mais les hommes ayant échoué à assurer la paix, la cyberpaix risque d'être très difficile à atteindre.

Liste des publications de référence

ANDRES, Richard B. ; SHACKELFORD, Scott J. « State Responsibility for Cyber Attacks : competing Standards for a Growing Problem », Georgetown Journal of International Law, 2011, vol. 42, n°4, p. 971.

BAUD, Michel. « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », Politique Étrangère, 2012, n°2, pp. 305-316.

[37]LOUIS-SIDNEY, B., préc., note 14, p. 79.
[38] FARWELL, James P. ; ROHOZINSKI, Rafal. « Stuxnet and the Future of Cyber War », *Survival: Global Politics and Strategy,* 2011, vol. 53, n°1, p. 23.
[39] SHACKELFORD, Scott J., préc., note 29, p. 217.
[40]ZEMANEK, Karl. « Armed attack », *Max Planck Yearbook of United Nations Law*, 2010, [en ligne].
[41]LITTLEWOOD, Jez. « Les discussions de 2011 sur la vérification de la Convention sur les armes biologiques ou à toxines », UNIDIR, 2010, p. 19, [en ligne].
[42]BAUD, M., préc., note 17, p. 305.
[43]*Id.*, p. 309.
[44]VENTRE, D., préc., note 2, p. 13.
[45]VENTRE, D., préc., note 27 , p. 86.

CENTER FOR SECURITY STUDIES. « Cyberguerre : concept, état d'avancement et limites », Politique de sécurité : analyses du CSS, n°71, 2010.

JOINT CHIEFS OF STAFF. « Joint Terminology for Cyberspace Operations », Département de la Défense, États-Unis, 2010.

LOUIS-SIDNEY, Barbara. « La dimension juridique du cyberespace », Revue internationale et stratégique, 2012, vol. 3, n° 87, pp. 72-82.

ROSCINI, Marco. « World Wide Warfare – Jus ad bellum and the use of cyber force », Max Planck Yearbook of United Nations Law, 2010, vol. 14, pp. 85-130.

SAMAAN, Jean-Loup. « Mythes et réalités des cyberguerres », Politique étrangère, 2008, n°4, pp. 829-841.

SHACKELFORD, Scott J. « From Nuclear War to Net War : analogizing Cyber Attacks in International Law », Berkeley Journal of International Law, 2009, vol. 57, n°1, p. 192.

VENTRE, Daniel. Cyberattaque et cyberdéfense, Paris, Lavoisier, 2011, 312 p.

VENTRE, Daniel. « La cyberpaix : un thème stratégique marginal », Revue internationale et stratégique, 2012, vol. 87, n°3, pp. 83-91.