Notions of war and peace within cyberspace

Sarah Gorguos (Master, Sherbrooke University)

July 2013, article n°III.10

War and peace are ancient notions, defined by international politics and law. Since the end of the 19th century, the development of information technologies has opened new perspectives[1]. During the 90s, cyberspace awareness rose, as a "space characterized by the use of electronics and the electromagnetic spectrum to sell, exchange or modify data, with computer systems and associated physical structures"[3]. Cyberspace poses unprecedented problems in politics and law, because it transcends conceptions of territory and borders, rendering obsolete the definitions of war and peace. This being said, cyberspace is ever more present in state cybersecurity strategies. Political resolve and state behavior with regards to cyberdefense greatly influence the way war and peace are assessed in this virtual setting. The problem is therefore the following: do the notions of war and peace make any sense in cyberspace? To answer this question it is necessary to study first the legal and political definitions of war and peace and, only after, why cyberspace is such a stake on both fields, from states' point of view.

1 –Inadequacy of the traditional legal and political definitions of war and peace, applied to cyberspace

State-centered legal definitions of war and peace, a hamper to the application of international law within cyberspace

An armed conflict exists as soon as « resorting to armed force occurs between several states »[4], peace being generally defined as the absence of conflict. Article 2, paragraph 4 of the United Nations Charter forbids, between member states, resorting to "[….] threat or use of force, either against territorial the integrity or the political independence

[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, traductionlibre 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.

Of any state [...]»[5]. An armed aggression must be linked to a state and is characterized by its intensity and by the fact that it threatens the territory of a State[6]. The applicability of international law in armed conflicts (jus ad bellum and jus in bello[7]) hinges on acts being linked to involved states[8], or the identification of the territory on which hostilities take place. The notion of border is paramount and the intensity of the conflict or the attack is of importance. This being said, a cyberconflict is characterized by it immaterial, de-territorialized aspect[10]: it is located out of state borders[11], because it can originate from, or be located within the territory of several states. A cyberattack is rapid and anonymous, and therefore difficult to link to a state[12]. The question of a cyberattack being a use of force generates large debates in doctrine, is not clearly settled by law and depends on the interpretation which is made of article 2 paragraph 4 of the Charter[13]. Moreover, the intensity and the damages of an attack are hard to assess[14]. For the same reason, the notion of armed attack is seldom used in the case of a cyberattack. Leaving the assessment task to the Security Council would amount to running the risk of letting international law be blocked by a veto. Therefore, current definitions of war and peace are a hamper in international law are a hamper on its application to cyberconflicts.

Larger political definitions, but ill-adapted to the evolution of the character of war : the need to adapt theory to practice

Outside the law, war can be defined as « […] a conflict between political groups, namely independent states, opposing armed forces during a long period »[15]. Here again, peace is understood to be the absence of war. In politics, definitions are no longer adapted to the new parameters of armed conflicts, such as cyberwar[16]. And it is gaining weight in the military strategies of states[17]. Its characteristics must therefore be assessed, according to the American Department of Defense, who claims military vocabulary is not adapted to cyberspace. Some define cyberconflicts as « […] a coordinated operation, led through cyberspace by a group with defined objectives, using information and communication systems »[19], which is much too vague. The definition task must take into account the inherent tension of the notion of cyberwar. The definition of cyberwar must enable the discrimination between military cyberattacks and others[20]. This definition must be sufficiently tight to

[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 UnitedNations 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, Citédans SHEEHAN, Michael, « Le caractèrechangeant 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.

The term cyberconflict not to be used to qualify all types of aggression[21]. But it must be loose enough to characterize all cyberwars, which don't always tick all the boxes of conventional war[22]. It must absorb all forms of "operations in computer networks"[23] and take into account all the aspects of cyberconflicts and not only its technological aspect[24]. Therefore, political definitions of war and peace must be re-adapted, and adequate definitions of cyberwar and cyberpeace must be designed.

2 –Cyberspace, a major challenge for war and peace

State cybersecurity, fuelling conflicts rather than peace

The study of the United State's or France's cybersecurity strategies proves that states prepare themselves to face cyberattacks and reply to them, in a kind of cyber-armament's race[27]. However, Russia and China have upheld the creation of a Conduct Code on the Internet[28]. Nonetheless, the cyberattacks which targeted Estonia in 2007 were linked to Russia[29], and China is one of cyberspace's greatest threats, for the United States[30]. State cybersecurity strategies must nonetheless operate in a defensive and offensive perspective, to compensate for the asymmetric nature of cyberconflicts and find a balance between resilience and disruption[31]. Limits, including legal ones, are necessary to master the consequences of these strategies. In the absence of adapted legal and political definitions of war and peace, those limits are impossible to set. Moreover, some states do not wish to master cyberspace[32]. State cybersecurity can therefore be a source of armed conflicts[33]. From a constructivist point of view, the nature of the anarchy which rules on the international system is determined by identities, perceptions, interests and the actions of the states[34]. Cyberspace is a competition system, as is shown by the cyber-armament race and the masked nature of cyberattacks, which are hardely ever linked to a state, and which don't constitute a direct confrontation. The challenge is therefore to prevent this "armed cyberpeace"[35] from slipping into an openly armed conflict.

Political and legal hampers to cyber-armament control

According to basic French Law, a cyberweapon is "a piece of equipment, an instrument, a computer program, [...] »[36]. What separates it from a harmless computer program is therefore the 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. Specifies the three types of possible operations.

[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*, June 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 », *BerkeleyJournal 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 », *InternationalOrganization*, 1992, vol. 46, n°2.

[35] Centre National de Ressources Textuelles et Lexicales, Définition de la paix, [en ligne], quoted in VENTRE, D., préc., note 27, p. 90.

[36] Nouveau Code pénal, art. 323-3-I.

with which it is created or used[37].
As is shown by the example of the Stuxnet virus[38], a cyberweapon is identifiable only once it is used, an intention being subjective a notion and hard to assess. It is possible to regulate cyberweapons through an analogy with nuclear weapons, for instance[39]. This regulation could only be possible *a posteriori*, once the weapon has been used, and cannot be autonomous: it hinges on the identification of a cyberattack, given that the weapon must be used with this intent. Cyberweapon control therefore stalls on the inadequacy of laws to cyberspace. To be deemed an armed aggression, the cyberattack must have caused serious human or material damage[40] and be linked to a state, both elements being difficult to establish. In addition, the impossibility of establishing the responsibility of anyone owning these weapons but not using them would entice states to acquire them and would hamper the ability to control, due to its downstream nature. Internationally, conventional armament control is blocked by state reluctance, as is stressed by the opposition to verification mechanisms from the 1975 biological arms convention[41]. It is very likely that cyberweapon regulation will run into the same problem, perhaps in a harder way.

Conclusion

The reason why cyberpeace must be upheld also enables us to conclude that notions of war and peace do bear a meaning in cyberspace. The real world and the virtual one permeate each other plentifully. Current conflicts include a cyber dimension[42]. Cyberattacks have actual consequences, as the 2007 Estonia attacks showed[43]. It is necessary to ensure cyberpeace, if only because of the extent to which societies rely on information technologies. However, those can be a tool for reconstructing peace, as they contribute to humanitarian operations[45]. But the virtual nature of cyberspace makes the threats which it contains difficult to assess, and the perception of their seriousness is altered. Defending cyberpeace requires legal and political definitions, so as to identify what could jeopardize it. But as men have failed to safeguard peace, cyberpeace may well be hard to reach.

References

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 andStrategy*, 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.