Polish Political Science Yearbook vol. 46 (1) (2017), pp. 271–280
DOI: 10.15804/ppsy2017117 PL ISSN 0208-7375

Mateusz Piątkowski
University of Łódź (Poland)

The Definition of the Armed Conflict in the Conditions of Cyber Warfare

Abstract: The paper is presenting the examination of the cyberwarfare phenomenon in its legal context. The cyberattacks are increasingly effective measures of modern combat and would probably become the most crucial dimension of forthcoming armed conflict. The role of the international humanitarian law is to determine whenever the cyberattack is reaching the threshold of an armed conflict. The aim of the article is to present the existing framework of *ius in bello* in terms of its temporal scope of applicability, especially in the light of the *Tallinn Manual on the International Law Applicable to Cyber Warfare*. It supported conclusion that the international law requires an revision of the armed conflict definition to sufficiently addressed the challenges arising from growing cyber activity.

Keywords: *armed conflict; international humanitarian law; cyberwarfare*

The Characteristic of the Modern Cyber Warfare

Introduction of the new technologies, especially the ground-breaking development of the Internet, computers, servers and networks have created a new reality. In the era when everything is connected by non-visual links the flow of information is delivered with unprecedented speed and unlimited range. The main legal ambiguity of the cyber-space lies in their *dual – use* character. While from the civilian perspective, the advantages of the Web are overwhelming, the opportunities for the military-use are even greater. From the states viewpoint increasing involvement in the process of building cyber-armed forces is attractive from various factors. Some of them are closely connected to the phenomena called *lawfare* – a new strategic doctrine apply both on the national and non-state entities level. According to this logic, the victory in further

armed conflict would be achieved not only by strict military means and methods. To obtain the battlefield advantage the belligerent sides will concentrated its military activity in the international humanitarian law grey scale. The specific types of actions will vary accordingly to circumstances. In order to covert its true operations, the state would use the non-state associated armed groups bearing no distinction, successfully bypassing the requirements of the article 1(2) Forth Hague Convention (e.g., see the conduct of the Crimea annexation). During the conflict of non – international character, the irregular fighters use the advantage of the principle of civilian immunity, by deliberate relocating its own military assets close to the inhabited areas (Dunlap, 2008, p. 149). Basing on the long-standing non-reprisal stance the of international humanitarian law and assuming the possible lawful conduct of the opponent party, the *lawfare* doctrine offered a rare opportunity to eliminate strategical or tactical asymmetry of the conventional armed forced by relatively low cost (Luban, 2011, p. 1).

Remarkably, the *cyberwarfare* (International Red Cross Committee, 2013) offered a rapid extension of the *lawfare* concept (Melzer, 2011, p. 4)[1]. Due to the characteristic of the network operations, the obliteration of the evidence linking the person responsible for the sponsor state is far more reachable than in 'conventional' environment. The *dual-use* characteristic of some Internet tools blurred the lines between the permissible and non-permissible countermeasures (Dunlap. 2011). From the viewpoint of international humanitarian law, one context of cyber conflict is especially alarming: when the certain network attacks would amount to the creation of legal term armed conflict?

Use of the Force During an Armed Conflict

From the centuries, the use of force generally require the existence of the kinetic force. The outcome was relying on a physical damages, destruction or injury. The new technologies on the battlefield just deployed the more advanced and sophisticated tools of a traditional way of combat (Lin, 2012). However, the phenomenon of the cyber-attack is a complete novelty. Certainly, it does not involve the use of kinetic force nor creates a psychical or visible outcome, although such possibility exists (see the actions of the Israel intelligence against the Iranian nuclear program) (Tabansky, 2011, p. 81; Denning, 2012, pp. 674–676). Even the 'outcome' of the network attack could be hardly recognized. The consequences might be stretchered in time, as the disruption of the financial system, the undermining of the political foundations or

[1] For the present purposes, the term 'cyberwarfare' refers to warfare conducted in cyberspace through cyber means and methods.

other inconvenience both in civil or military activity (Estonia 2007, Georgia 2008, Ukraine 2014, USA 2016). However, the scale of *cyberdevastation* would in some circumstances amount to the effects of the *conventional* armed conflict. In this place is vital to make a distinction between the various terms used in international public law. The armed activity of the state or non- state group would in some circumstances be classified as an *use of force* (art. 2(4) of the United Nations Charter), *armed attack* that justify the self-defence reaction (art. 51 UN Charter) and finally the phrase *attack* as described on the ground of art. 49 I Additional Protocol to Geneva Conventions of 1977, which is an element of the *armed conflict* regarding international humanitarian law (Schmitt, 2012, p. 285). There is no clear parallelism between those concepts (Waxmann, 2011). Not every *use of force* is simultaneously the evidence of the existing *armed conflict*- e.g., the shoot-down of Russian fighter jet by Turkish Air Forces in September 2015 (Peagler, 2014, p. 421). Similarly, single *use of force* would not amount to the *armed attack* in the meaning of the art 51 UN Charter (Grevais, 2012, p. 543; Roscini, 2014, p.70–71).

The Definition of the Armed Conflict.

The precise definition of the armed conflict in the international humanitarian law is nowhere to be found in *ius in bello* treaties. Nevertheless, the concept is used commonly since Forth Geneva Convention of 1949[2]. It replaces the term 'war' from two reasons. Firstly, the scope of the above-mentioned phrase is generally associated with conflicts of the international character (Boot, 2002, p. 9). The state practice before 1949 indicates the specific unwillingness among the nations, to call hostilities as an act of war (Mrazek, 2010, p. 98). During the clashes between the Japan and the Soviet Union in the late 30`s, the number of deceased and injured soldiers raised beyond the number of 30 000, yet none of the belligerent-parties called those 'skirmishes' as an element of war between the fighting states (Simon Fan, 2016, p. 205). Later, some justifications for sending own troops abroad were more sophisticated, e.g. humanitarian intervention in order to protect own companions in other nation (the USSR invasion against Poland September 17, 1939) or to secure the claimed area of influence (the Chinese-Japanese War, Italian invasion against Ethiopia in 1935) (Kawaguchi, 2003, pp. 166–167). None of those actions were preceded by the formal declaration

[2] In addition to the provisions which shall be implemented in peacetime, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them. *See* Convention (1949).

of war, despite the formal requirements of the Third Hague Convention (Alder, 2012, pp. 48–50). To avoid such situations when proclaiming the *state of war* is a subjective decision of the involved states, the Geneva Convention proposed a new and objective concept of *armed conflict* (Pictet, 1952, p. 32; International Red Cross Committe, 2008, p. 1)[3]. The other factor arise from the bitter experiences of the civil wars occurred in the mid-war Europe, especially the brutal conduct of non-international conflict in Spain during the 1936–1939 (Perna, 2006, p. 39–41). The international community realized that the term 'war' was only applicable in the case of inter-state hostilities, while the international humanitarian law lacked a specific instrument regulating the internal disturbances involving the use of the armed force. However, the direct formulation of the armed conflict definition had been left to the international law experts and jurisprudence. In 1995 the International Criminal Tribunal for Former Yugoslavia in one of the first judicial decisions established a generally accepted interpretation of the term[4]. In 2013, under the directorship of the Michael Schmitt, in the *Tallinn Manual on the International Law Applicable to Cyber Warfare* NATO experts proposed an amendment definition of the cyber international armed conflict (see more details in chapter below). Nevertheless, the questions of armed conflict threshold and the distinction between the *use of force* and *armed conflict* remain disputed.

The Meaning of *Attack* in the Light of the International Humanitarian Law

What kind of network attack would amount to the act of armed conflict in the light of international humanitarian law? As it was mentioned earlier, the cyber operations are not involving *per se* the use of kinetic force. According to the article 49(1) of the

[3] A State can always pretend when it commits a hostile act against another State, that it is not making war, but merely engaging in a police action, or acting in legitimate self-defence. The expression "armed conflict" makes such arguments less easy. Any difference arising between two States and leading to the intervention of armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the existence of a state of war. *See* Pictet. J (1952).

[4] On the basis of the foregoing, we find that an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State. International humanitarian law applies from the initiation of such armed conflicts and extends beyond the cessation of hostilities until a general conclusion of peace is reached; or, in the case of internal conflicts, a peaceful settlement is achieved. Until that moment, international humanitarian law continues to apply in the whole territory of the warring States or, in the case of internal conflicts, the whole territory under the control of a party, whether or not actual combat takes place there. *See Prosecutor v. Dusko Tadic*. (1995).

I Additional Protocol, the provision stipulates that the term *attack* generally refers to violence arising from offensive or defensive acts of combat operations (Richardson, 2011, p. 9). This includes all types of attack, while the specific mean is not necessarily merely causing a visible psychical destruction (Liivoja et al, 2016, p. 606). As pointed by Laurie Blank, the use of nuclear, chemical or biological weapons is fulfilling the definition described on the grounds of the article 49(1) of the I Additional Protocol (Blank, 2014). Despite their non-kinetic character, those means of combat are creating a 'violent' outcome e.g., on human health. This conclusion is an important remark in the context of cyberwarfare, indicating that the use of specific weapons during the armed hostilities must imply the effect similar to the conventional tools of fighting like physical destruction or harmful injury (Richardson, 2011, p. 178). It would be helpful in this place to present the practical example, allowing to better understand the interplay between the phenomenon of cyberwarfare and international humanitarian law. Let us imagine the aerial bombardment directed against the power plant servicing for military purposes. The bomb fall, the object is destroyed and in consequence is the disruption of the energy flow. If trough the network attack (e.g., DDOS, virus or any other hacking methods) the computers systems failure forces plant to stops its operation, in result the outcomes would be *similar* to those created by the aerial strike (despite not being kinetic *per se)* (Schmitt, *International Law Studies* 2008, p. 94)[5]. This method of analysing, which focuses on the consequences of the attack has been called an effect-based approach. The aforementioned test is currently considered to be the most appropriate in terms of cyberwarfare. It sufficiently draws a distinction between the acts of war (e.g., the shutdown on energy power for the military purpose) involving the violence and the actions of propaganda, information or psychological warfare (Radziwill, 2015, p. 177). The previous method of measuring the scale of the network attack (the instrument-based approach) had been dismissed as an impractical by not taking into account the outcomes of the cyber strike (Simmons, 2014, p. 53–61). The third type of test been known as target – based – approach. According to some states armed forces military doctrine, the cyber-attack against any of the components of so – called critical infrastructure (e.g., nuclear plants, early warning radar systems) triggers the possibility of conventional armed response (Melzer, 2011, pp. 14–16). The last test is criticized for being too broad and inherently creating

[5] Referring back to the requirement of violence, and its development in Additional Protocol I, cyber operations can, therefore, qualify as "attacks," even though they are not themselves "violent," because they have "violent consequences." A cyber operation, like any other operation, is an attack when resulting in death or injury of individuals, whether civilians or combatants, or damage to or destruction of objects, whether military objectives or civilian objects. *See* Schmitt. M.N. (2008).

a possibility of the unproportional retaliation, despite relatively harmless network strike. It is also vital to underline that some network operations would be limited to interfere or disrupt the operational capabilities of other computer systems – such an example of *the cyber-attack* in terms of common language is revoked when adhering it to the circumstances of the Ukraine and Estonia. The outcomes of those actions are difficult to measure in the scope of the article 49(1) of the I Additional Protocol (Geiss, 2013, p. 644). Not all of them are imminently linked to the emerge of the physical harm, which is essential to qualify such act as *attack* in the light of the international humanitarian law (Kodar, 2012, p. 112). M. Norris proposed the remodeling of the *cyber-attack* definition by adjusting the concept of *neutralization* which may eventually by applicable in situations related to the computers systems disturbances not amounting to physical damages (Morris, 2013).

The Threshold of the Armed Conflict

As described before, not every use of armed forces is constituting a state of armed conflict (Assada, 2012, p. 66). The ICTY *Tadic* definition lacks precision in this aspect when adhering it to the international armed conflicts. The question became apparent in the circumstances of the low – intensity armed operations or isolated incidents. According to the J. Pictet's (1952, p. 32) commentary do the Geneva Convention, the provisions of laws of war apply in any case of armed confrontation between the state, irrespective of the actual scale of death and destruction. After the Second World War some experts highlight the need for analyzing the idea of *animus belligerent* – the states reaction to the specific use of force (Kelsen, 2003, p. 27). According to the concept, the belligerent parties should recognize their action as an act of war to exercise their *intent* to actually wage war. This notion had been criticized, as considered as a step back in the development of international humanitarian law by applying again the model of subjective approach to the concept of armed conflict (Dinstein, 2011, pp. 14–15). The majority of experts agreed that sporadic, isolated and short term incidents are not considered to reach the threshold of the armed conflict. The Ethiopia-Eritrea Claims Commission highlight that the limited skirmishes between the armed forces (especially border guard units) are not amounting to act of armed conflict, despite the loss of life during such incidents (Eritrea-Ethiopia Claims Commission, 2006, p. 465) [6]. Another legal ambiguity lies in the context of the unilateral

[6] Localized border encounters between small infantry units, even those involving the loss of life, do not constitute an armed attack for purposes of the Charter. *See* Reports on International Arbitral Awards.

armed actions such as shoot down of Russian fighter jet above the Syrian air space by Turkish F-16s or Israelian Air Forces strike against nuclear installation in Syria which lacked both the intensity and *animus belligerent* element (Watkin, 2016, pp. 57–58). Examination of the South Korean warship sinking in 2010 conducted by the Institute of International Law lead to the conclusion that despite the scale of destruction, the incident was not sufficient to meet a threshold of armed conflict (International Law Association, 2010, p. 31).

The New Definition

The definition of the armed conflict proposed by the *Tallinn Manual* is clearly referring to the widely accepted and well established ICTY`s definition (Schmitt, 2013, p. 79)[7]. The novelty of the proposal introduced the aspects of cyber operations described as hostilities. *The cyber armed conflict* would be constituted when the specific acts conducted via network attacks will reach the scale similar to the effects of conventional armed attack and eventually include the destruction or other harmful effects. Nevertheless, in my opinion, the contemporary binding definition of the international armed conflict should be reinforced by the introduction of the additional elements, including the gravity, scale, intensity and some element of addressing the existence of the war-waging *intent* on both sides of conflict. There should at least some at least factual 'understanding' among adversaries about the specific act of warfare (e.g the armed attack should be followed by the act of resistance). Those elements should sufficiently addressed the challenges arising from the unilateral network attacks. The main idea of the proposed definition would still manifest the requirement of *violence* emerging as a consequence of the specific *network attack.* The sufficient gravity and adequate scale of the cyber military operations will operate as a test of the distinction between the acts that fall under the category of armed conflict and those which are only the examples of the *use of force.* Similar approach had been manifested by some experts during the discussion over the second edition of *Tallin Manual* (Schmitt, 2017, p. 383). Even though, as described above, in the history of the international disputes one might invoked that there been multiple situations when the one – sided military actions involving the significant destruction and even the loss of life have not been constituting the state of armed conflict, due to lack certain *intent* of both sides to accept the incident as an act of armed conflict. To conclude, I define the international armed conflict in cyberspace as 'the armed interaction between the states, achieving

[7] An international armed conflict exist whenever there are the hostility which may include or be limited to cyber operations, occurring between two or more states. *See* Schmitt. M.N. (2013).

level of respective intensity and exercising their intent to wage an offensive or defensive acts (including the means of cyberwarfare). To adapt this definition to the realities of contemporary international relationship I observed that probably only the cyber attack directed against Ukrainian power grid (executed in December 2015) would be classified as an example of armed attack in terms of international humanitarian law. The strike caused similar effects to conventional use of force and forced the energy shortage on Eastern Ukraine (Kittichaisaree, 2017, p. 156). Nevertheless, the incident was not followed by the armed response – a factor, which negates the element of armed conflict. Officially, the authorities were unable to establish and prove the jurisdictional link between the hackers and the foreign state.

Conclusion

The realities of the cyberwarfare provide enough evidence to support the conclusion that the existing definitions of the international armed conflict might require an implementation of the additional elements. After 20 years since the ICTY's *Tadic* decision had been ruled the number of unilateral armed operations raised significantly. The majority of those acts were conducted by the states, while the existing interpretation of the term 'international armed conflict' had not been comprehensive enough to resolve the challenges arising from the one – sided combat operations, that may cause destruction and loss of life. It is possible to predict that in the future, the state – sponsored hackers group would eventually launch a covert action against the military, economic and political structures against its international opponents. The gravity and consequences of some *cyber-attacks* would eventually reach the threshold of the international armed conflict. However, it is vital for international peace and stability to make the effective distinction between the acts of war and the actions not amounting to the level of conventional hostilities. The introduction of the supplementary elements (intensity, intent, and gravity) to the already existing definition of the armed conflict will improve the international humanitarian law ability to steer successfully through the grey-scale legal area of low-intensity armed conflict and cyber operations. Finally, the newly accepted definition would be successful in limiting the negative consequences arising from the *lawfare* doctrine. Clarifying when *use of force* is amounting to the level of the armed conflict in the cyberspace, will consequently triggers the applicability of the international humanitarian law with all its privileges and duties regulating the conduct of the belligerents parties.

References:

Alder, M.C. (2012). *The Inherent Right of Self-Defence in International Law*. Dorodrecht: Springer.

Asada, M. (2012). "The Concept of 'Armed Conflict' in International Armed Conflict: Non – International Armed Conflict". In M.E. O`Connell (Eds.), *What Is War?: An Investigation in the Wake of 9/11* (pp. 51–69). Leiden: Martinus Nijhoff Publishers.

Blank, L. (2014). "Cyberwar/Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace. Cyberwar: Law & Ethics for Virtual Conflicts". *Emory Legal Studies Research Paper,* 14, pp. 1–34.

Boot, M. (2002). *Genocide, Crimes Against Humanity, War Crimes: Nullum crimen sine lege and the Subject Matter Jurisdiction of the International Criminal Court.* Antwerpen: Intersentia.

Convention (IV) relative to the Protection of Civilian Persons in Time of War. Geneva, 12 August 1949.

Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907.

Denning, D.E. (2012)." Stuntex: What Has Changed". *Future Internet*, 4, pp. 672–687.

Dinstein, Y. (2011). *War, Agression and Self – Defence*. Cambridge: Cambridge University Press.

Dunlap, C.J. (2008). "Lawfare Today: A Perspective". *Yale Journal of International Affairs*, 3(1), pp. 146–154.

Dunlap, C.J. (2011). "Perspectives for Cyber Strategists on Law for Cyberwar". *Strategic Studies Quarterly*, 5, pp. 81–99.

Kodar, E. (2012). "Applying The Law of Armed Conflict to Cyber Attacks: From the Martens Clause to I Additional Protocol". *ENDC Proceedings*, 12, pp. 107–132.

Geiss. R. (2013). "Cyber Warfare: Implications for Non-international Armed Conflicts". *International Law Studies*, 62, pp. 627–645.

Gervais, M. (2012). "Cyber Attacks and the Laws of War". *Berkeley Journal of International Law*, (30)525, pp. 525–575.

Hiroshe Kawaguchi, K. (2003). *A Social Theory of International Law*. Leiden: Martinus Nijhoff Publishers.

"International Commitee of the Red Cross. (2008). How is the Term >>Armed Conflict<< Defined in International Humanitarian Law?". *International Committee of the Red Cross (ICRC) Opinion Paper.*

"International Commitee of the Red Cross. What limits does the law of war impose on cyberattacks?" (2013). *International Committee of the Red Cross*. Retrieved from: https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm.

International Law Assosication. (2010). "The Hague Conference". *Use of Force - Final Report on the Meaning of Armed Conflict in International Law.*

Kelsen, H. (2003). *Principles of International Law*. New Jersey: The Law Book Exchange.

Liivoja, R., & Leins, R,. & McCormack, T. (2016). "Emerging Technologies of Warfare". In. R. Liivoja et al. (Eds). *Routledge Handbook of International Law of Armed Conflict*. New York: Routledge.

Lin, H. (2012). "Cyber conflict and international humanitarian law". *International Review of the Red Cross*, 94(886), pp. 515–531.

Luban, D. (2011). "Carl Schmitt and the Critique of Lawfare". *Georgetown Public Law and Legal Theory Research Paper,* 11, pp. 1–14.

Melzer, N. (2011). *Cyberwarfare and International Law*. Geneva: UNIDIR Resources.

Mrazek, J. (2010). Armed Conflicts and the Use of Force. *Czech Yearbook of International* Law, 1, pp. 97–109.

Norris, M.J. (2013). "The Law of Attack in Cyberspace: Considering the Tallinn Manual's Definition of 'Attack' in the Digital Battlespace". *Inquiries Journal/Student Pulse*, 5(10). Retrieved from: http://www.inquiriesjournal.com/a?id=775.

Kittichaisaree K. (2017). *Public International Law of Cyberspace*. Cham: Springer.

Peagler, J. (2014). "The Stuntex Attack: A New Form of Warfare and the (In)Applicability of Current International Law". *Arizona Journal of International & Comparative Law*, 31(2), pp. 399–432.

Perna, L. (2006). *The Formation of the Treaty Rules Applicable in Non-international Armed Conflicts*. Leiden: Martinus Nijhoff Publishers.

Pictet, J. (1952). *Commentary, Geneva Convenion of 12 August 1949*. Geneva: International Red Cross Committee.

Prosecutor v. Dusko Tadic aka "Dule" (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction), IT-94–1, International Criminal Tribunal for the former Yugoslavia (ICTY), 2 October 1995.

Radziwill, Y. (2015). *Cyber-Attacks and the Exploitable Imperfections of International Law*. Leiden: Brill.

"Eritrea-Ethiopia Claims Commission (2006): Partial Award–Jus ad Bellum, Ethiopia's Claims 1–8". *International Legal Materials, 45*(2), pp. 430–435

Richardson, J. (2011). "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield". *J. Marshall Journal of Computer & Info Law*, 29(1), pp. 1–29.

Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press.

Schmitt, M.N. (2008). "Cyber Operations and the Ius In Bello Key Issues". *International Law Studies*, 87, pp. 90–110.

Schmitt, M.N. (2012). ">Attack< as a Term of Art in International Law: The Cyber Operations Context". *Proceedings of the 4th International Conference on Cyber Conflict,* pp. 283–293.

Schmitt, M.N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Schmitt, M.N. (2017). *Tallin Manual 2. 0 on International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press

Simmons, N. (2014). "A Brave New World: Applying International Law of War to Cyber Attack". *Journal of Law and Cyber Warfare*, 4(1), pp. 53–61.

Simon, Fan. C. (2016). *Culture, Institution, and Development in China: The Economics of National Character*. Oxon: Routledge.

Tabansky. L. (2011). "Basic Concepts in Cyber Warfare". *Military and Strategic Affairs*, 3(1), pp. 75–92.

Watkin, K. (2016). *Fighting at the Legal Boundaries: Controlling the Use of Force in Contemporary Conflict*. Oxford: Oxford University Press.

Waxmann, M.C. (2011). "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)". *The Yale Journal of International Law,* 36, pp. 421–459.

Author

Mateusz Piątkowski

University of Łódź, Faculty of Law and Administration. Contact details: ul. S. Kopcińskiego 8/12, 90-033 Łódź, Poland; e-mail: piatkowskimat@gmail.com.