European Journal of Political Science Studies
ISSN: 2601 - 2766
ISSN-L: 2601 - 2766
Available on-line at: www.oapub.org/soc

DOI: 10.46827/ejpss.v4i1.937 Volume 4 | Issue 1 | 2020

CYBER-ATTACKS AS AGGRESSION CRIMES IN CYBERSPACE IN THE CONTEXT OF INTERNATIONAL CRIMINAL LAW

Gianpiero Greco[i]
Ministry of the Interior,
Department of Public Security,
State Police, Italy
orcid.org/0000-0002-5023-3721

Abstract:
The recent situation in the world shows that cyber-attacks could be one of the most dangerous threats to international peace and security. Offensive operations in cyberspace present unique challenges to the international legal order, which are faced by the international community. While it is consensual that international law applies to cyberspace, the debate about the qualification of cyber-attacks as fundamental crimes under International Criminal Law is still ongoing and has not produced definitive answers. Addressing the implications of transnational cyber threats from the perspective of International Criminal Law will perhaps require a further amendment of the Rome Statute. After briefly illustrating how cyber-attacks are commonly linked in the debate to war crimes, genocide and crimes against humanity, a more detailed analysis will be devoted to the admissibility of cyber-attacks as crimes of aggression, this being the crime most recently defined and, perhaps, the most controversial.

Keywords: International law; hacker; computer crimes; cyber warfare; cyber threats

1. Introduction

The recent situation in the world shows that cyber-attacks could be one of the most dangerous threats to international peace and security (Shackelford, 2009). The very nature of offensive operations in cyberspace presents unique challenges to the international legal order. Currently, the debate on cyber-attacks takes place mostly in the contexts of *ius ad bellum* and *ius in bello*. While it is consensual that international law applies to cyberspace, the debate regarding the qualification of cyber-attacks as fundamental crimes under International Criminal Law has been less intense and fruitful. After briefly illustrating how cyber-attacks are commonly linked in the debate to war crimes, genocide and crimes against humanity, a more detailed analysis will be devoted

[i] Correspondence: email gianpierogreco.phd@yahoo.com

to the admissibility of cyber-attacks as crimes of aggression, this being the crime most recently defined and, perhaps, the most controversial.

2. Cyber-attack characteristics

The new regulation is often developed through the application of reasoning by analogy by existing legislative bodies. However, the nature of cyber-attacks presents unique challenges. For this reason, proceeding by analogy can be exceptionally complicated especially due to two manifest characteristics of cyberspace: anonymity and deterritorialization (Chaumette 2018). Roscini (2014) argues that there are three levels of proof necessary to attribute a cyber-attack to a specific State for international law to be applicable: "*First, the computer or computers, or the server or servers from which the operations originate, must be located; secondly, it is the individual who is behind the operation that must be identified; and thirdly, what must be proven is that the individual acted on behalf of a State so that his conduct is attributable to it*" (Ohlin et al. 2015, p. 220).

Cyber-attacks challenge the traditional principle of territoriality of international law. The geolocation of the attack is, however, a fundamental step in defining the context of international criminal conduct, for example in the assessment of the existence of aggression, in the definition of a conflict such as the 'International Armed Conflict' or the 'Non-International Armed Conflict' or in the assessment of the territorial jurisdiction of the International Criminal Court (Chaumette, 2018).

Attribution is the ability to identify who attacked a computer network and from what location. The process of attributing a cyber-attack is arguably the most difficult challenge. First, it is not always easy to trace from an IP address to an end-user, as IP addresses are often associated with hundreds of end-users. Second, hackers are generally able to disguise their identity. Furthermore, as Ophardt (2010) notes, cyber-attacks can occur in several States, such as in the case of botnets that are collections of devices connected to the Internet which, infected with malware, are controlled by the botmaster to carry out DDoS (Distributed Denial of Service) attacks: *"Botnets are not geographically limited; the malware that creates them moves freely across national borders […]. Internet traffic has been specifically designed to travel on the fastest possible route. This path is not necessarily the same as the geographically most direct path".* are collections of devices connected to the Internet which, infected with malware, are controlled by the botmaster to carry out DDoS (Distributed Denial of Service) attacks.

All this leads to the even more problematic question of the link between the hacker and the State or organization that hires the hacker. Another challenge arises from the fact that most cyber-attacks are not 'State-sponsored', but conducted by 'Non-State Actors' groups, by groups of individuals or individuals acting alone. Then, cyber weapons, while having highly destructive potential, are a cheap weapon in the arsenal of the 'Non-State Actors' and can easily be created by highly skilled hackers. However, International Law is hardly applicable to these categories of actors (Faga, 2017).

3. Cyber-attacks and debate on International Law

The absence of a definition of 'threat of use of force' or 'use of force' in the United Nations Charter (1945) led to a problem of interpretation. This gap was filled with the adoption of United Nations General Assembly Resolution 3314 (1974) on the definition of aggression, by which States agreed by consensus that 'force' means 'armed force', within the meaning of Article 2, paragraph 4, of the Charter of the United Nations. The answer to the question of whether a computer operation falls within the scope of Article 2, paragraph 4, depends on which of the three main analytical approaches to understand the nature of the use of armed force is accepted. The tool-based and the objective-based approaches have been criticized for being too restrictive one and too broad the other, while the approach that received the most support has been the effects-based approach (Roscini, 2014).

This perspective is also reflected in the definition of cyber-attack provided by the Tallinn 2.0 Handbook - the most authoritative non-binding study on the applicability of international law to cyber warfare - according to which a cyber-attack is "*a cyber operation, both offensive and defensive, which can reasonably cause injury or death to persons or damage or destruction of objects*" (Rule 92, Tallinn Handbook 2.0) (Schmitt, 2017). This definition implies that to qualify as a use of force, a cyber-operation must be comparable in scale and effects to those of a kinetic attack (Rule 69, Tallinn Manual 2.0). Therefore, in assessing whether a computer operation is equivalent to a use of force, the fact that the force was acted on by computer means is irrelevant. In this regard, in its advisory opinion, the International Court of Justice established that Article 2, paragraph 4, of the United Nations Charter, applies to "*any use of force, regardless of the weapons employed"* (advisory opinion on the legality of the threat or use of nuclear weapons of 1996, p. 22). Therefore, the assimilation of some cyber-attacks with armed force allows the United Nations Security Council to act under Chapter VII and for States to react in self-defence (Article 51 of the United Nations Charter) (Schmitt, 2017).

The debate on the applicability of international humanitarian law has led to the fundamental conclusion that, despite the absence of specific provisions on international humanitarian law, this body of law is flexible enough to be relevant to the cyber operations that occur both during the International Armed Conflict and the Non-International Armed Conflict. In particular, the cardinal principles of ius in bello (i.e. the principles of distinction, precaution, and proportionality) are applicable (Chaumette, 2018).

4. Cyber-attacks in the context of International Criminal Law

Offensive operations in cyberspace are usually neglected from an International Criminal Law point of view; therefore, the debate regarding the qualification of cyber-attacks as fundamental crimes has been less intense. However, if on the one hand, it is less controversial to consider cyber-attacks as war crimes or crimes against humanity, on the

other hand, the qualification of a cyber-attack as genocide or crime of aggression is still a source of discussion (Chaumette, 2018).

The United Nations Group of Governmental Experts concluded that acts committed by computer means can be qualified as war crimes (as in Article 8 of the Rome Statute, 2002) if they meet the objective (actus reus) and subjective (mens rea) requirements (Rule 84, Tallinn Handbook 2.0) and provided that there is a belligerent link, i.e. such attacks are part of ongoing conflict (Ambos, 2015; Schmitt, 2017).

For crimes against humanity, the contextual element is that the underlying conduct - in this case, a cyber-attack - is committed "*as part of a widespread or systematic attack directed against any civilian population*" and "*in accordance with or following of a state or organizational policy aimed at committing this attack*" (article 7, Rome Statute, 2002). As remote as the possibility is, a cyber-attack could be a new means of perpetrating crimes against humanity, such as murder or extermination.

Regarding the link between cyber-attacks and the crime of genocide, experts from the Tallinn Handbook 2.0 concluded that "*a cyber-attack would occur before the launch of genocide, as it would be used to identify individuals belonging to the target group. It would intervene in the preparatory phase of the genocide but could not qualify as genocide*" (Chaumette, 2018). Furthermore, as Vagias (2016) observes, a cyber-attack could be a form of public and direct incitement to commit genocide, as prohibited by the Convention for the prevention and suppression of the Crime of Genocide. While the incitement was qualified as an act of genocide both in the Statute of the International Criminal Tribunal for the former Yugoslavia and in that of the International Criminal Tribunal for Rwanda, this is no longer the case in the Rome Statute (2002), where the incitement to commit genocide is instead a mode of responsibility (Vagias, 2016). According to Article 25 of the Rome Statute (2002), anyone who contributes to the commission of a crime can also be held responsible, either by instigation or by complicity.

5. Cyber-attacks as crimes of aggression

In 2002, the International Criminal Court was established by the international treaty - the Rome Statute - as the only permanent court responsible for the pursuit of individual responsibility for fundamental crimes under the International Criminal Law. The crime of aggression was listed in Article 5, paragraph 1, letter d), among the heinous crimes falling within the jurisdiction of the International Criminal Court. However, no consensus was reached among the delegates on its definition, nor on the trigger mechanism and how to exercise the Court's jurisdiction over the crime and these issues were left to the subsequent Review Conference which was convened in Kampala, Uganda, in 2010. The Conference led to the approval by the Assembly of States Parties of the so-called "Kampala Compromise", but only later a series of amendments to the Rome Statute (2017) was activated which finally defined the crime of aggression (sanctioned by article 8 bis, Rome Statute) and the conditions for exercising jurisdiction over this crime (in articles 15 bis and ter, Rome Statute).

While this development may appear as an enlargement of the judicial capacity of the International Criminal Court to prosecute individuals for further basic crime, many scholars have expressed concern that the crime of aggression will have strict applicability to modern conceptions of warfare (Miller, 2014). Several issues related to cyber-attacks seem to emerge. Article 8 bis, paragraph 1, of the Rome Statute provides for a definition of the crime of aggression as *"the planning, preparation, initiation or execution, by a person capable of effectively exercising control or directing the political or military action of a State, of an act of aggression which, due to its character, gravity and scope, constitutes a manifest violation of the Charter of the United Nations".* This wording makes it explicitly impossible for the International Criminal Court to prosecute individuals who act alone or who can lead a group of 'Non-State Actors'. Beyond that, states themselves are likely to hire private hackers to conduct cyber operations, as highly technical skills are required to carry out attacks. However, as anticipated, the issue of attribution makes it difficult to demonstrate the link between the State that recruited the hacker and the latter. Even if this were possible, the hacker would still not be responsible. In the case of the other three fundamental crimes, if the hacker's facilitation triggers individual criminal liability pursuant to Article 25 of the Rome Statute, this is not the case with aggression crimes. Article 25, paragraph 3 bis, requires that the provision applies only to people acting as leaders. Furthermore, Article 8 bis, paragraph 1, already sets a high standard for which attacks will be sufficient for prosecution, as they must constitute a 'manifest' violation of the United Nations Charter. The field of application of this formulation is deliberately restrictive, to avoid attacks of a minor entity to be pursued.

Article 8-bis, paragraph 2, of the Rome Statute is a textual replica of Articles 1 and 3 of Resolution 3314 on the definition of aggression. This could represent an obstacle, given that the definition of aggression concerns only the traditional use of force, which applies only to States and which is based on traditional concepts such as territorial integrity. According to Kocibelli (2017), the wording of the article has two important limitations. First, the postponement of the qualification of international crime to the United Nations General Assembly resolution of 1974 - when contemporary and hybrid forms of warfare were not contemplated - means that an outdated definition has crystallized into treaty law, thus preventing further customary developments. Also, acts of aggression are defined by the way they are carried out (instrumental approach), rather than by their consequences (effects approach), making it difficult for cyber-attacks to fall within the scope of the article (Kocibelli, 2017).

Miller (2014) argues instead that Kampala's definitions can be flexibly interpreted by judges of the International Criminal Court to include the cyber-attacks. Besides, according to Article 4 of the United Nations General Assembly Resolution 3314 on the definition of aggression, the United Nations Security Council can determine which other acts constitute aggression, thus possibly allowing cyber-attacks to fall into this category. Concerning Article 3 of the resolution of the United Nations General Assembly, Papanastasiou (2010) also supports the same broad vision and argues that assuming that *"a cyber force could form part of a state's armed forces, it is very easy for cyber-attacks to fall*

within the legal scope of acts (a), (b), (c), (d) and (e) of aggression […]. Regarding letter g), cyber-attacks are perpetrated by hackers, who can be considered mercenaries".

A further restriction on the qualification of cyber-attacks as crimes of aggression derives from Articles 15 bis and ter which state that the International Criminal Court has jurisdiction only if a State commits aggression against another State and that the law applies only to States who have effectively ratified the Kampala amendments, i.e. 35 (not including Italy) of the current 123 States Parties. As a further limit the applicability of the new crime, the possibility was finally provided for each ratifying State to disassociate itself from the amendments at any time (so-called 'opt-out clause').

6. Conclusions

Offensive operations in cyberspace present unique challenges to the international legal order, which are faced by the international community. Most of these efforts have been collected in the Tallinn Handbook and the Tallinn 2.0 Handbook which, while authoritative, are non-binding academic studies. However, they are a sign of the willingness of States to regulate cyberspace. As explained in paragraph 5 above, the debate within the International Criminal Law, about the qualification of cyber-attacks as fundamental crimes is still ongoing and has not produced definitive answers. The qualification of cyber-attacks as crimes of aggression is particularly critical. Depending on the approach they take, legal experts still have differing opinions on the subject. According to Miller (2014) "*at least for the time being, practical and jurisdictional barriers are likely to prevent the application of the crime of aggression in the context of cyber-aggression. Consequently, several other methods should be pursued simultaneously by international groups to promote peaceful cyberspace*". Addressing the implications of transnational cyber threats (as well as other hybrid forms of warfare) from an International Criminal Law perspective will perhaps require further modification of the Rome Statute. However, as shown by the process that led to the approval of the Kampala Compromise (Kreß & Von Holtzendorff, 2010; Miller, 2014) and subsequent amendments (Whiting, 2017), this seems for the moment a remote possibility.

Conflict of interest

The author declares no conflicts of interest.

References

Ambos, K. (2015). International criminal responsibility in cyberspace. In *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing.

Amendments to the Rome Statute of the International Criminal Court on the Crime of Aggression (2017). Retrieved from https://asp.icc-cpi.int/iccdocs/asp_docs/RC2010/AMENDMENTS/CN.651.2010-ENG-CoA.pdf

Charter of the United Nations and Statute of the International Court of Justice (1945). Retrieved from https://www.un.org/en/charter-united-nations/.

Chaumette, A. L. (2018). International Criminal Responsibility of Individuals in Case of Cyberattacks. *International Criminal Law Review, 18*, 1-35.

Faga, H. P. (2017). The implications of transnational cyber threats in international humanitarian law: analysing the distinction between cybercrime, cyber-attack, and cyber warfare in the 21st century. *Baltic Journal of Law & Politics*, *10*(1), 1-34.

Kocibelli, A. (2017). Aggression, From Cyber-Attacks to ISIS: Why International Law Struggles to Adapt. *Michigan Journal of International Law, 39*.

Kreß, C., & Von Holtzendorff, L. (2010). The Kampala compromise on the crime of aggression. *Journal of International Criminal Justice*, *8*(5), 1179-1217.

Miller, K. L. (2014). The Kampala Compromise and Cyberattacks: Can There Be an International Crime of Cyber-Aggression? *Southern California Interdisciplinary Law Journal, 23*, 217.

Ohlin, J. D., Govern, K., & Finkelstein, C. (Eds.). (2015). *Cyber war: law and ethics for virtual conflicts*. OUP Oxford.

Ophardt, J. (2010). Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. *Duke Law & Technology Review, 3*, 30.

Papanastasiou, A. (2010). Application of International Law in Cyber Warfare Operation. https://dx.doi.org/10.2139/ssrn.1673785

Rome Statute of the International Criminal Court (2002). Retrieved from http://www.cirpac.it/pdf/testi/Statuto%20di%20Roma%20della%20Corte%20Penale%20Internazionale.pdf

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

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Shackelford, S. J. (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. *Berkeley Journal of International Law, 27*, 192-198.

United Nations General Assembly Resolution 3314 on the Definition of Aggression (1974). Retrieved from https://legal.un.org/avl/pdf/ha/da/da_ph_e.pdf

Vagias, M. (2016). The Territorial Jurisdiction of the ICC for Core Crimes Committed Through the Internet. *Journal of Conflict and Security Law*, *21*(3), 523-540.

Whiting, A. (2017). Crime of Aggression Activated at the ICC: Does it Matter? Retrieved from https://www.justsecurity.org/49859/crime-aggression-activated-icc-matter/.