Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi • Cilt 26, Sayı 2, Aralık 2020, ISSN: 2529-0142, ss. 1063-1078 • DOI: 10.33433/maruhad.798304

ARAŞTIRMA MAKALESİ / RESEARCH ARTICLE

War Crimes and Individual Criminal Responsibility Arising Out of Cyber Operations

Savaş Suçları ve Siber Operasyonlardan Doğan Bireysel Cezai Sorumluluk

Yunus Emre GÜL*

Abstract

The types of individual criminal responsibilities are listed in the Rome Statute Article 25(3). Individuals or organized groups who conduct cyber operations during armed conflicts have an individual criminal responsibility derived from their acts. They may commit war crimes by conducting cyber operations that reach a certain level of violence, however, even if the operation does not constitute a war crime *per se*, perpetrators might still be responsible for their actions. In line with this, how an individual criminal responsibility occurs arising out of those operations is examined in this article.

Keywords: Individual Criminal Responsibility, Rome Statute, Cyber Operations, Violence, War Crimes.

Öz

Bireysel cezai sorumluluk türleri Roma Statüsü Madde 25(3)'te listelenmiştir. Silahlı çatışmalar sırasında siber operasyonlar gerçekleştiren bireyler veya organize gruplar, eylemlerinden doğan bireysel cezai sorumluluğa sahiptirler. Bu kişiler belirli bir şiddet eşiğine ulaşan siber operasyonlar düzenleyerek savaş suçları işleyebilirler; ancak bu operasyon bizatihi savaş suçu teşkil etmese dahi, failler eylemlerinden sorumlu olabilirler. Bu doğrultuda, söz konusu operasyonlardan doğan bireysel cezai sorumluluğun nasıl ortaya çıktığı bu makalede incelenmektedir.

Anahtar Kelimeler: Bireysel Cezai Sorumluluk, Roma Statüsü, Siber Operasyonlar, Şiddet, Savaş Suçları.

Introduction

Individuals witnessed significant developments in the international law related to the Law of Armed Conflict (LOAC) in the 20th century. Although Clausewitz claims that 'to introduce into the philosophy of war itself a principle of moderation would be an absurdity'[1] in the first half of the 19th century, the world has changed after having suffered two world and several civil wars between

* LLM at King's College London, Department of Law, London, United Kingdom, E-Mail: yunus_emre.gul@kcl.ac.uk

1 Clausewitz, 2007, p 14.

Makale Gönderim Tarihi: 22.09.2020
Yayına Kabul Tarihi: 29.10.2020

1915-1945. Experiences of the Second World War led to the establishment of the Nuremberg Trials in 1945-1946, and this became an initial phase of the International Criminal Law that provides to judge war criminals. Developments in International Criminal Law have continued after Nuremberg Trials, and International Criminal Court was established by the Rome Statute of the International Criminal Court (the Rome Statute) on July 17, 1998, and on July 1st, 2002, the Rome Statute of the International Criminal Court (ICC), entered into force.

Whilst Article 8 of the Rome Statute states that International Criminal Court has jurisdiction over war crimes, a person who commits a war crime is individually responsible for his/her actions under Article 25 of the Rome Statute. In the first part of this essay, definitions of armed conflict, war crimes and cyber operations and how an individual incurs criminal responsibility for these operations will be addressed. In the second part, different forms of individual criminal responsibilities, which are set out between Article 25(3)(a)-(f) of the Rome Statute, namely commission, instigation, assistance, complicity, incitement to genocide, attempt and abandonment, will be explained. In addition, how each of these kinds of criminal responsibilities incurs by cyber operations will be discussed in the context of war crimes.

I. Definitions

A. Armed Conflict

War crimes are only be committed in case of armed conflict. There are two types of armed conflicts according to Geneva Conventions; International and Non-International. While Common Article 2 of Geneva Conventions lays out international armed conflicts by stating that the 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', in respect of non-international armed conflicts Common Article 3 sets out that each Party to the conflict is bound to apply provisions stated in the Article 'in the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties'. Although both articles contain the term of 'armed conflict', neither of the Conventions has a definition for it.

Armed conflict is defined in the *Tadic* Case as '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'.[2] While the first part of the definition, 'a resort to armed force between States', is applicable to international armed conflicts, the second part is applied to non-international armed conflicts. The determining factor between them is the status of actors. Hence, an international armed conflict exists only when there are states as belligerent parties, non-international armed conflict occurs between 'governmental authorities and organized armed groups or between such groups within a State'.

There are two conditions for the existence of an international armed conflict. The first one is that, as Common Article 2 of 1949 Geneva Conventions and *Tadic* Case stated above underline, if at least

2 Tadic Case, 2 October 1995, para 70.

one side of conflict is a state, the conflict will be deemed 'international'. The second one is, if an armed group conducts its acts under the control of a state against another state, the nature of conflict will be considered 'international'. While the International Court of Justice (ICJ) adopts the 'effective control'[3] criterion, the International Criminal Tribunal for the former Yugoslavia (ICTY) adopts 'overall control'[4] which represents a lower threshold while determining the control of a state over an armed group.

Two conditions, intensity and organization, must be met in order to define an armed conflict as 'non-international'.[5] In terms of intensity, the threshold should be higher than 'the level of riots, internal disturbances or tensions, or isolated or sporadic acts of violence', and an armed conflict should be 'protracted'.[6] In terms of organization criterion, if a group has 'a set of structures or mechanisms, whatever those may be, that are sufficiently efficient to ensure the coordination necessary to carry out an attack directed against a civilian population' and 'sufficient means to promote or encourage the attack', then the group will meet organization criterion.[7] However, it is important to assess both of these criteria case by case basis.

B. War Crimes

After the conflict has been classified as International or Non-International Armed Conflict, all acts which are conducted in association with it are governed by the LOAC. The Rome Statute defines war crimes in Article 8 as, inter alia, "serious violations of the laws and customs applicable in international armed conflict" and "serious violations of the laws and customs applicable in an armed conflict not of an international character". Accordingly, if an act violates the LOAC, and has been laid out as war crime according to Article 8 of the Rome Statute, it will be named as 'war crime' resulting in individual criminal responsibility under treaty or customary international law.[8] In line with this definition, even though not every breach of the LOAC causes to individual criminal responsibility, such violations which are specifically criminalized pursuant to Article 8 of the Rome Statute will be characterized as 'war crimes' and examined in this essay.[9] Also, there is no difference in means of warfare such as guns, knives or cyber operations has been or to be used in a war crime. If the consequences of an act occur defined outcome of a war crime as regulated in Article 8 of the Rome Statute, a perpetrator will be liable for this act.

Although more than fifty kinds of war crimes are listed in the Rome Statute Article 8, it might be handier to focus on general points rather than listing all of them here. First of all, all crimes in Article 8 have one objective and one subjective element in common. Whilst the objective element is

3 Nicaragua Case, 27 June 1986, para 115.

4 Tadic Case, 15 July 1999, para 145.

5 Tadic Case, 7 May 1997, para 562; Pictet, 1952, p 49-50.

6 Tadic Case, 7 May 1997, para 562; Pictet, 1952, p 50; Bemba Case, 21 March 2016, para 140; Roma Statute Art 8(d).

7 Katanga Case, 7 March 2014, para 1119.

8 Cryer, 2010, p.267; Triffterer & Ambos, 2016, p 305.

9 Triffterer & Ambos, 2016, p 305.

'the conduct took place in the context of and was associated with an armed conflict', the subjective element is 'the perpetrator was aware of factual circumstances that established the existence of an armed conflict'.[10] Secondly, there are four categories of war crimes under Article 8 of the Rome Statute as stated by Dormann below;[11]

- Grave breaches which have been defined in the four Geneva Conventions such as 'extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly' according to Article 8(2)(a)(iv).
- Other serious violations of treaty or customary law which are applicable to international armed conflicts such as 'intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects or widespread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated' according to Article 8(2)(b)(iv).
- Serious violations of Geneva Conventions which are applicable to non-international armed conflict such as 'violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture' according to Article 8(2)(c)(i).
- Other serious violations of the laws and customs applicable in armed conflicts not of an international character such as 'intentionally directing attacks against the civilian population as such or against individual civilians not taking direct part in hostilities' according to Article 8(2)(e)(i).

C. Cyber Operations and Responsibility

Owing to rapid developments in technology throughout the 21st century, cyber space has become the fifth domain, in addition to land, sea, air and space, through which cyber operations and attacks are actively conducted in order to harm adversaries and gain military advantage by states. However, as stated in Additional Protocol-I to the Geneva Conventions of 1949 (AP-I) Article 35, '[i]n any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited'[12]. In such regard, there are limitations in carrying out operations against adversaries and going beyond such limitations may result in individual criminal responsibility.

Before defining cyber operations, the meaning of a military operation must be clarified. Military operation refers to 'any movements, manoeuvres and other activities whatsoever carried out by the armed forces with a view to combat'.[13] However, when an operation reaches a certain level of violence,

10 Dormann, 2003.

11 Dormann, 2003, p 343-345.

12 Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3.

13 Sandoz et al., 1987, para 2191.

it is defined as a military attack. In other words, "all acts that are designed, intended, or 'reasonably expected to cause injury or death to persons or damage or destruction to objects'" are considered as a military attack.[14] For this reason, although all attacks are a kind of operation, it does not mean that any operation will be automatically deemed as an attack.

Secondly, it is essential to keep in mind the distinction between cyber operations other than cyber attacks. While the former means that 'the employment of cyber capabilities to achieve objectives in or through cyberspace'[15], the latter is 'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[16] The difference between these two terms is the occurrence of a certain level of violence. Thus, as stated in Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Tallinn Manual), 'a cyber operation that alters the running of a SCADA system controlling an electrical grid and results in a fire qualifies. Since the consequences are destructive, the operation is an attack'.[17] Hence, a cyber attack is a specific kind of cyber operation that results in violent consequences.

Both members of the armed forces and civilians may be responsible for conducting cyber operations, these operations, however, must be 'in the context of and associated with the armed conflict' in order to incur responsibility for war crimes.[18] For this reason, individuals who are 'engaged in purely criminal cyber operations or malicious cyber activities unrelated to the on-going international or non-international armed conflict' cannot bear individual criminal responsibility for war crimes.[19]

In addition, committing a war crime requires a serious violation of the LOAC. For this reason, responsibility for war crimes as perpetrator in terms of Article 25(a) of the Rome Statute requires a certain level of violence, which is only possible with cyber-attacks. Although other types of cyber operations do not constitute war crimes by themselves, they may lead to responsibility due to a war crime that takes place. For example, a virus to be leaked into the controlling system of an electrical grid may disrupt the system's functions and thereby, result in excessive collateral damage that constitutes war crimes according to Article 8(2)(b)(iv) of the Rome Statute, and perpetrator(s) will be responsible from this act according to Article 25(3)(a) of the Rome Statute. On the other hand, even if a cyber operation does not result in violent consequences, individual criminal responsibility may incur. For instance, an individual who shares racist posts in order to incite others to commit genocide bears criminal responsibility derived from this cyber operation despite the fact that he/she does not commit violent acts according to Article 25(3)(e) of the Rome Statute.

14 Heinegg, 2015, para 10.

15 Tallinn Manual, Glossary.

16 Tallinn Manual, Rule 92.

17 Tallinn Manual, Rule 92, Commentary para 3.

18 Tallinn Manual, Rule 84, Commentary para 3.

19 Ibid.

II. Individual Criminal Responsibility for War Crimes and Cyber Operations

A. Commission

Article 25(3)(a) of the Rome Statute sets out three different ways of committing crimes: individual, jointly with another person or through another person.

1. Individual Commission

A perpetrator can commit the physical perpetration of a crime with his own initiative.[20] In a narrower sense, it can be argued that a person who commits a crime without taking any assistance or influence from anyone is responsible for that crime individually.[21] However, in a broader sense, a crime can be committed by a person who individually fulfils statutory elements of the crime and named as 'principal' even though other parties make contributions to the commission of the crime.[22]

Individual commission of war crime by a cyber attack is well exampled in Tallinn Manual as;

> 'Consider a case in which a member of the armed forces responsible for cyber operations accesses an industrial control system in the enemy State during an armed conflict. Using the access, the operator creates overpressure in the sole natural gas pipeline providing fuel to a town in the enemy's territory with the intent of depriving the population of the gas. The attack ruptures the pipeline and consequently the civilian population loses its only source of power, thereby foreseeably resulting in deaths due to harsh winter conditions'.[23]

Thus, a person who conducts a cyber attack by having a criminal intent (*dolus directus*) will be individually responsible because of his/her act. Also, even if he/she is not a member of armed force, the result would be same because while the existence of armed conflict is necessary to define a specific act as 'war crime', the status of person does not relieve his/her responsibility from war crimes.

2. Joint Criminal Enterprise (JCE)

Joint crimes are conducted 'by groups of individuals acting in pursuance of a common criminal design'.[24] Thus, in this type of responsibility, the act is committed within the framework of the common plan, and every co-perpetrator bears a responsibility for the whole crime because of making essential contribution to it.[25]

20 Tadic Case, 15 July 1999, para 188.

21 Eser, 2002, p 789.

22 Eser, 2002, p 789.

23 Tallinn Manual, Rule 84, Commentary para 6.

24 Tadic Case, 15 July 1999, para 191.

25 Ambos, 2016, article 25, Commentary para 8, p 988; Werle, 2007, p 958.

There are three types of joint commissions which are basic, systemic and extended (respectively JCE I, II and III).[26] JCE I requires to conduct the crime in accordance with common design, and co-perpetrators must share a same intent to realise the crime.[27] JCE II requires committing a crime 'in running a system of ill-treatment of prisoners in a concentration camp or a detention facility'.[28] JCE III concerns an act that exceeds the framework of the common plan and causes a responsibility of co-operators because of 'natural and foreseeable consequences' of it.[29] While these three types of responsibility have same *actus reus*, each of them has different *mens rea*.

In terms of *actus reus*, three objective criteria including plurality of persons, existence of a common plan and essential contribution to the crime must be met to bear joint responsibility. First, although they do not need to be organised, at least two people must have joint control over the crime.[30] Second, the crime must be carried out in accordance with a common plan, design or purpose. [31] Third, each perpetrator must make essential contribution to a crime in order to realise the objective elements of it.[32] What makes a contribution essential is based on whether a plan can be completed without such contribution.[33] The term 'jointly' supports requiring essential contribution level because if the co-perpetration is understood in a broad manner 'as by accepting the mutual attribution of contributions made in a functional division of labour for the accomplishment of the crime', then it will be no difference between co-perpetration and just assisting to a crime.[34] Also, it is not necessary to contribute the crime in execution stage 'but also, depending on the circumstances, at its planning or preparation stage, including when the common plan is conceived'.[35] For this reason, in *Tadic* Case, it was decided that 'all persons who participate in the planning, preparation or execution of serious violations...are individually responsible for such violations'.[36]

ICTY determines different *mens rea* element for each type of JCE. JCE I requires to have 'the intent to perpetrate a certain crime (this being the shared intent on the part of all co-perpetrators)'.[37] JCE II requires to have not only personal knowledge of the system of ill-treatment but also 'the intent to further this common concerted system of ill-treatment'.[38] Although JCE III requires to have an intention and contribution as common elements of co-perpetration, it also needs two elements that '(i) it was foreseeable that such a crime might be perpetrated by one or other members of the group

26 Ambos, 2016, article 25, Commentary para 9, p 988; Werle, 2007, p 959-960.
27 Tadic Case, 15 July 1999, para 196.
28 ibid para 202; Werle, 2007, p 959-960.
29 ibid para 204; Brđanin Case, 3 April 2007, para 431.
30 Lubanga Case, 29 January 2007, para 343; Tadic Case, 15 July 1999, para 227.
31 Lubanga Case, 29 January 2007, para 343; Tadic Case, 15 July 1999, para 227.
32 Lubanga Case, 29 January 2007, para 346; Tadic Case, 15 July 1999, para 227; Brđanin Case, 3 April 2007, para 430.
33 Werle, 2007, p 962.
34 Eser, 2002, p 790.
35 Lubanga Case, 1 December 2014, para 469.
36 Tadic Case, 15 July 1999, para 190.
37 ibid para 228.
38 ibid.

and (ii) the accused willingly took that risk.'[39] for having responsibility over acts which goes beyond the common plan.

In 2010 a malware named Stuxnet was leaked into Iran's nuclear facility at Natanz. The virus affected SCADA systems of the facility and caused to destroy a lot of centrifuges. Although, neither the scale of destruction caused by the attack nor attackers are officially declared, it was claimed that the virus was 'created and built by the NSA in partnership with the CIA and Israeli intelligence'.[40] Now, consider a branch of intelligence service that commonly planned and conducted a cyber attack against SCADA system of a nuclear facility in an armed conflict and caused extensive destruction of property which is a war crime according to article 8(2)(a)(iv). All perpetrators have joint responsibility arising out of this attack according to Article 25(3)(a). However, not only people who conduct this operation bear responsibility but also people who have a role at the planning stage of the crime are responsible for this operation. Thus, technical units of intelligence service, who designed this malware and played an active role to accomplish this cyber attack, may be responsible based on co-perpetration.[41]

3. Intermediary Perpetration

In this type of perpetration, the executor is used by the indirect perpetrator as a tool without being aware of criminal responsibility for his actions, and the latter has control over the crime because of his higher knowledge or superior willpower.[42] This control can be carried out by two ways; 'either over the will of the physical perpetrators, considered thereby incapable or irresponsible; or over the organization'.[43]

In order to have responsibility as principal over the crime, three elements are required which were listed in Katanga Case: An indirect perpetrator (i) 'must exert control over the crime whose material elements were brought about by one or more persons', (ii) ' must meet the mental elements prescribed by article 30 of the Statute and the mental elements specific to the crime at issue', and (iii) 'is aware of the factual circumstances which allow the person to exert control over the crime'.[44]

Cyber space significantly eases committing crimes even by children. Consider a twelve-year-old child who hacks into the controlling system of a dam in an armed conflict by being unaware of the consequences of his action owing to will of his father.[45] His father may bear individual criminal responsibility for this act.

39 Ibid.

40 Bamford, 2013.

41 Tallinn Manual, Rule 84, Commentary para 10.

42 Katanga Case, 30 September 2008, para 495; Eser, 2002, p 793.

43 Chaumette, 2018, p 27.

44 Katanga Case, 7 March 2014, para 1399.

45 Dinniss, 2014, p 1.

B. Instigation

Instigation means to 'prompt another person to commit an offence'.[46] A person who orders, solicits or induces the commission of war crime is individually responsible from that act according to Article 25(3)(b) of the Rome Statute. Ambos defines soliciting a crime as, *inter alia*, 'urging, advising, commanding, or otherwise inciting another to commit a crime', and inducing a crime as 'enticement or urging of another person to commit a crime'.[47] However, ordering a crime is narrower than these two types of instigation because it requires to have superior subordinate relationship, in other words 'a position of authority'.[48] Although it is not necessary to have a formal relationship, a person in position must have a power to instruct the perpetrator to commit a crime by using his/her authority.[49] In other words, his/her authority must reach a level that 'would compel another to commit a crime in following the accused's order'.[50] However, obeying the order does not relieve the criminal responsibility of the perpetrator.

Mens rea of the crime requires 'the awareness of the substantial likelihood that a crime will be committed in the execution of that instigation'.[51] Eser describes *mens rea* of that crime with his 'double intent' theory:

> '[F]irst, with regard to his own conduct, the instigator must exert his influence with intent and knowledge. This means that the intent of the instigator must be directed at causing the principal to commit the crime. Secondly, the instigator must presuppose that the principal will carry out the crime in a state of mind required by the Statute'.[52]

That is why, a superior, who is a head of branch of intelligence service that will conduct a cyber attack as stated above, has individual criminal responsibility for this attack despite of the fact that he does not conduct any violent act himself/herself. Even if he/she does not give an order to commit a war crime but the perpetrator does, the superior, who already 'knew or, owing to the circumstances at the time, should have known the forces were committing or about to commit' a war crime, bears individual criminal responsibility for this operation due to not to take feasible precautions in order to prevent it.[53] For this reason, a superior, who claims that cyber operations require a technical expertise and he/she does not have such knowledge, cannot relieve his/her 'responsibility for exercising control over their subordinates'.[54]

46 Kordic Case, 17 December 2004, para 27.
47 Triffterer & Ambos, 2016, p 1003.
48 Nchamihigo Case, 18 March 2010, para 188.
49 Akayesu Case, 2 September 1998, para.483; Kordic Case, 17 December 2004, para 28.
50 Semanza Case, 20 May 2005, para 361.
51 Kordic Case, 17 December 2004, para 32.
52 Eser, 2002, p 797.
53 Rome Statute Art 28(a).
54 Tallinn Manual, Rule 85, Commentary para 10.

C. Assistance

An individual, who aids, abets or otherwise assists to commit a war crime by having a purpose of facilitating the commission of it, is criminally responsible according to Article 25(3)(c).

Although 'providing means' is clearly stated in the article, *actus reus* element of the crime should be held in a more inclusive way. It requires to carry out acts in order to practically assist, encourage or grant moral support by being aware of the fact that they have a substantial effect on the commission of the crime.[55] While the aider does not have control over the commission, and the crime can still be committed without that contribution, his contribution must have a causal relationship with the outcome.[56] For example in *Delalic* Case, it was concluded that the role of the assistant in 'publicly justifying and defending the purpose and legality of the camp', and his 'participation in the classification and releasing of prisoners' constitute aiding and abetting.[57]

The practice of ICTY and ICC differs when applying *mens rea* of the crime. While the former does not require to have an 'intent' to commit a crime, the latter requires to facilitate the commission of a crime. According to the ICTY, if a person knows the intention of the perpetrator, this mere knowledge is enough to conclude that he/she is responsible for the crime as an aider or abettor. [58] Also, it is not necessary to know the precise crime, but 'if he is aware that one of a number of crimes will probably be committed, and one of those crimes is in fact committed, he has intended to facilitate the commission of that crime, and is guilty as an aider and abettor'.[59] On the other hand, in *Mbarushimana* Case, it was stated by the ICC that 'article 25(3)(c) of the Statute requires that the person acts with the purpose to facilitate the crime; knowledge is not enough for responsibility under this article'.[60]

Aiding and abetting refers to different occasions. While aiding means to give assistance to someone, abetting would include to facilitating 'the commission of an act by being sympathetic thereto'.[61] As it is stated in Tallinn Manual, if a person gives 'the malware or information regarding vulnerabilities that was necessary to enable the war crime to be committed', he/she may bear a responsibility derived from that act in terms of aiding', but if an individual posts 'online exhortations to continue the slaughter of civilians of a particular religious group during an armed conflict', he/she may bear a responsibility for abetting with regard to the effectiveness of these exhortations.[62]

55 Vasiljević Case, 25 February 2004, para 102; Furundzija Case, 10 December 1998, para 235; Blaskic Case, 29 July 2004, paras 46,49; Tadic Case, 7 May 1997, para 688.

56 Werle, 2007, p 969; Triffterer & Ambos, 2016, p 1003-4.

57 Delalic Case, 20 February 2001, para 356.

58 Furundzija Case, 10 December 1998, paras 236, 249. Blaskic Case, 29 July 2004, para 50.

59 Furundzija Case, 10 December 1998, para 246.

60 Mbarushimana, 16 December 2011, paras 274, 281.

61 Akayesu Case, 2 September 1998, para 484.

62 Tallinn Manual, Rule 84, para 15.

D. Complicity

A person who knows the intent of the group is criminally responsible for contributing the commission of the crime in any other way except those stated in Article 25(3)(c). Thus, the application of Article 25(3)(d) is limited to a crime by a group of persons acting with a common purpose.

Regarding the actus reus of the crime, the accomplice must contribute a crime that is committed or attempted by a group of persons acting with a common purpose.[63] A group is formed by at least three persons who have a common purpose to commit a crime, and the accomplice contributes to realize that purpose in any other way which does not fall in Article 25(c). [64] However, ICC renders to limit the scope of the article by determining the contribution as significant that has 'a bearing on the occurrence of the crime and/or the manner of its commission'.[65] While determining the contribution as significant, the Pre-Trial Chamber argues several factors;

> '(i) the sustained nature of the participation after acquiring knowledge of the criminality of the group's common purpose, (ii) any efforts made to prevent criminal activity or to impede the efficient functioning of the group's crimes, (iii) whether the person creates or merely executes the criminal plan, (iv) the position of the suspect in the group or relative to the group and (v) perhaps most importantly, the role the suspect played vis-à-vis the seriousness and scope of the crimes committed. These factors are not a substitute for assessing the suspect's contribution to a crime, but they can assist in the assessment.'[66]

Regarding *mens rea*, article 25(d) offers two choices in addition to intention; first, 'the aim of furthering the criminal activity or criminal purpose of the group', and second 'the knowledge of the intention of the group to commit the crime'. According to the first alternative, the participant may have some 'special intent' by aiming to advance criminal activity or criminal purpose.[67] However, according to the second alternative, the participant is aware of the intention of the group that is already directed to a specific crime.[68]

Consider a person who introduces more complex malware than those used by perpetrators in order to ease the crime which will be committed by the perpetrator. Although the crime can be committed without these malware, he/she is responsible for his/her act which aims to ease the commission. Also, a person who permits to the perpetrator to use his computer and conduct cyber attack via his/her IP address by being aware of the intention of the perpetrator, may bear responsibility for complicity according to Article 25(3)(d).

63 Werle, 2007, p 970; Eser, 2002, p 802.

64 Werle, 2007, p 970; Eser, 2002, p 802.

65 Katanga Case, 7 March 2014, paras 1632-3.

66 Mbarushimana, 16 December 2011, para 284.

67 Triffterer & Ambos, 2016, p 1015; Eser, 2002, p 803.

68 Triffterer & Ambos, 2016, p 1015; Eser, 2002, p 803.

E. Incitement to Genocide

A person who 'directly and publicly incites others to commit genocide' is responsible because of his actions even if genocide does not occur according to Article 25(3)(e).[69] Incitement should not be understood 'as a mere causing another person to commit a crime, but by provoking, arousing, exhorting, inspiring, urging on, or otherwise promoting the other person to engage in genocidal activities'.[70]

It is important to note that the incitement must be direct and public. The 'direct' element of incitement requires urging or provoking another person to engage in a genocidal act immediately.[71] Although it does not need to be comprehended by everyone, if the relevant audience of such indictment gets the message very well despite using 'euphemistic, metaphorical or otherwise coded language', then it will constitute direct incitement.[72] For this reason, it should be determined case by case basis and taking the culture of the country into consideration.[73] The 'public' element refers to calling for criminal action to a number of persons 'in a public place or to members of the general public at large by such means as the mass media, for example, radio or television'.[74]

Mens rea of the crime requires having an intent to directly and publicly incite others to commit genocide. The perpetrator desires to create a particular state of mind among his/her audience by having 'the specific intent to commit genocide, namely, to destroy, in whole or in part, a national, ethnical, racial or religious group, as such'.[75] Although Ambos claims that 'there must be a specific causal link between the act of incitement and the main offence'[76], Eser rightly states that the relationship is 'volitional' between the incitement and genocide, since even if the incitement failed to produce the result expected by the perpetrator, he/she will still be responsible.[77]

Social media is an important platform to directly and publicly incite others to commit genocide. A person, who shares racist posts and spreads fake news by having an 'intent to destroy, in whole or in part, a national, ethnical, racial or religious group'[78], is responsible even if his/her incitement does not create a material effect. Also, even if a perpetrator shares these posts by using another state's server that is not party to the Rome Statute, but the targeted audience lives in a country that is party to the Rome Statute, then the jurisdiction of the ICC over a perpetrator can be established.[79]

69 Akayesu Case, 2 September 1998, para 561.

70 Eser, 2002, p 805.

71 Akayesu Case, Trial Judgement, 2 September 1998, para 557; Triffterer & Ambos, 2016, p 1017.

72 Werle, 2007, p 972.

73 Akayesu Case, 2 September 1998, para 558.

74 Akayesu Case, 2 September 1998, para 556; Triffterer & Ambos, 2016, p 1016.

75 Akayesu Case, 2 September 1998, para 560; Ruggiu Case, 1 June 2000, para 14.

76 Triffterer & Ambos, 2016, p 1017.

77 Eser, 2002, p 804-805; Akayesu Case, 2 September 1998, para 562.

78 Roma Statute Art 6.

79 Vagias, 2016, p 538-539.

F. Attempt and Abandonment

According to article 25 (f), if a person commences the execution of a crime "by means of a substantial step, but the crime does not occur because of circumstances independent of the person's intentions", he/she will be responsible because of attempting a crime. However, if that person completely and voluntarily gives up committing a crime, then he/she will not bear responsibility.

Attempt refers to a situation where the crime does not occur because of reasons on which the perpetrator does not have control. Regarding actus reus, the perpetrator must commence the execution of the crime by taking a significant step which aims to conclude the crime.[80] Although Ambos states that 'the harm is absent'[81] in an attempt, this is a false premise. For example, an attempt to genocide, after it began and some people are killed, it can be stopped by the interference of the United Nations (UN). That is why not the absence of the harm, but the absence of the desired conclusion makes an act to be named as 'attempt'. Mens rea of the crime is to have an intention as stated in article 30 of the Rome Statute.

As stated above, even if the effects of cyber attack initiated by a branch of intelligence service are prevented by technical experts of the facility, and it does not cause to occur any violence, perpetrators will be responsible for that act on the basis of attempting a war crime. However, if they produce a malware to conduct cyber attack, but they do not take any further step, this cannot be rendered as the commencement of a crime.

Abandonment refers to a situation in which while the crime may be completed, the perpetrator does not conclude its deed without any external intervention. *Actus reus* of the abandonment is to prevent the conclusion of a crime. *Mens rea* of it is to give up the criminal purpose completely and voluntarily. If a branch of intelligence service voluntarily gives up carrying out its cyber attack further because of expected violent consequences on civilian people, this action will be held as abandonment, and they will not bear any responsibility.

Conclusion

After the development of new technologies, committing war crimes and vanishing traces to excuse individual responsibility became easier. However, this does not prevent *lex lata* from being applied to current cases.

The first step is development of cyber forensics for war crimes. Although it is possible to find useful evidence for war crimes by using the record of network events, for most military actions, it would become rather difficult. Most preprogrammed attacks for particular times are scattershot and usually ineffective in what are often highly fluid international crises. Although it is not easy tracing, routers

80 Eser, 2002, p 811-12; Triffterer & Ambos, 2016, p 1020.

81 Triffterer & Ambos, 2016, p 1020.

store recent connection data, and this must be accessed as quickly as possible, to obtain connection information from critical-infrastructure networks which often store this kind of data.

The second step would be attribution. However, proving that a country is responsible for an attack is harder than proving that a single hacker is responsible, since just because attacks originate within a country does not mean that its government is responsible.

The final step would be to judge a person who has a criminal responsibility arising out of attributed cyber operations. At this point, a person does not bear responsibility only for those acts which reach certain level of violence, but he/she bears responsibility by instigation, assistance etc. Therefore, not only cyber attacks, which represent a high threshold, but also cyber operations may incur an individual criminal responsibility. Although there is no precedent on this issue, it is important to be aware of the fact that cyber operations may cause violent consequences and be prepared before the occurrence of such consequences.

BIBLIOGRAPHY

I. Primary Sources

Treaties

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3.

Rome Statute of the International Criminal Court (entered into force 1 July 2002) 37 ILM 1002 (1998); 2187 UNTS 90

Cases

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) (Judgment) [1984] ICJ Rep 392

Prosecutor v Anto Furundzija (Trial Judgment) ICTY-95-17/1-T (10 December 1998)

Prosecutor v Callixte Mbarushimana (Decision on the confirmation of charges)

Prosecutor v Dario Kordic and Mario Cerkez (Appeal Judgement) ICTY-95-14/2-A (17 December 2004)

Prosecutor v Dusko Tadic (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) ICTY-94-1 (2 October 1995)

Prosecutor v Dusko Tadic (Trial Judgment) ICTY-94-1-T (7 May 1997)

Prosecutor v Dusko Tadic (Appeal Judgement) ICTY-94-1-A (15 July 1999)

Prosecutor v Germain Katanga and Mathieu Ngudjolo Chui (Decision on the confirmation of charges) ICC-01/04-01/07 (30 September 2008)

Prosecutor v Germain Katanga (Judgement pursuant to article 74 of the Statute) ICC – 01/04-01/07 (7 March 2014)

Prosecutor v. Georges Ruggiu (Trial Judgment) ICTR-97-32-1 (1 June 2000)

Prosecutor v Jean-Paul Akayesu (Trial Judgment) ICTR-96-4-T (2 September 1998)

Prosecutor v Jean-Pierre Bemba Gombo (Judgment pursuant to Article 74 of the Statute) ICC-01/05-01/08 (21 March 2016)

Prosecutor v Laurent Semanza (Appeal Judgment) ICTR-97-20-A (20 May 2005)

Prosecutor v Mitar Vasiljevic (Appeal Judgment) ICTY-98-32-A (25 February 2004)

Prosecutor v Radoslav Brđanin (Appeal Judgment) ICTY-99-36-A (3 April 2007)

Prosecutor v Siméon Nchamihigo (Appeal Judgement) ICTR-2001-63-A (18 March 2010)

Prosecutor v Tihomir Blaskic (Appeal Judgement) ICTY-95-14-A (29 July 2004)

Prosecutor v Thomas Lubanga Dyilo (Decision on the confirmation of charges) ICC-01/04-01/06 (29 January 2007)

Prosecutor v Thomas Lubanga Dyilo (Appeal Judgement) ICC-01/04-01/06 A 5 (1 December 2014)

Prosecutor v Zejnil Delalic, Zdravko Mucic, Hazim Delic and Esad Landžo (Appeal Judgement) ICTY-96-21-A (20 February 2001)

II. Secondary Sources

Books, Book Chapters, Articles

Chaumette AL, 'International Criminal Responsibility of Individuals in Case of Cyberattacks' (2018) 18 International Criminal Law Review 1

Cryer R and others, *An Introduction to International Criminal Law and Procedure* (Cambridge University Press 2010)

Dinniss HH, *Cyberwarfare and the Laws of War* (Cambridge University Press 2014)

Dormann K, 'War Crimes under the Rome Statute of the International Criminal Court, with a Special Focus on the Negotiations on the Elements of Crimes' in von Bogdandy A and Wolfrum R (eds) Max Planck Yearbook of United Nations Law Volume 7 (Martinus Nijhoff Publishers 2003)

Eser A, 'Individual Criminal Responsibility Mental Elements —Mistake of Fact and Mistake of Law' in Cassese A and others (eds) *The Rome Statute of the International Criminal Court: A Commentary Volume I* (Oxford University Press 2002)

Pictet JS (ed), *Commentary I Geneva Convention For the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* (ICRC 1952)

Sandoz Y and others (eds), Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (ICRC 1987)

Schmitt M (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press 2017)

Triffterer O and Ambos K (eds), The Rome Statute of the International Criminal Court A Commentary (Third Edition, Beck/Hart 2016)

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

von Clausewitz C, *On War* (Howard M and Paret P trs, Oxford University Press 2007)

Werle G, 'Individual Criminal Responsibility in Article 25 ICC Statute' (2007) 5 Journal of International Criminal Justice 953

Electronic Sources

Bamford J, 'NSA Snooping Was Only the Beginning. Meet the Spy Chief Leading Us Into Cyberwar' (*Wired*, 2013) < https://www.wired.com/2013/06/general-keith-alexander-cyberwar/> accessed 3 January 2020

von Heinegg WH, 'Proportionality and Collateral Damage' (*OPIL*, October 2015) <https://opil.ouplaw.com/view/10.1093/law:epil/978.019.9231690/law-978.019.9231690-e2166> accessed 17 December 2019