FRASER, ANETA MARIANNA

Büntetőjogi Tanszék
Témavezető: dr. Ambrus István habil. egyetemi docens
DOI: https://doi.org/10.56966/2024.8.Fraser

CYBERCRIME FROM THE PERSPECTIVE OF THE CONTROL OVER THE CRIME THEORY IN INTERNATIONAL CRIMINAL LAW: NEW CHALLENGE, ESTABLISHED SOLUTIONS?

Abstract

The concept of paradigm can be applied not only to broad areas such as the distinction between positivism, post-positivism, interpretivism, but also to narrower issues such as accepted definitions within a particular branch of law. One such example is the decision of the International Criminal Court to reject the joint criminal enterprise doctrine and to adopt the German 'control theory'. The adoption of a different theoretical framework has resulted in a shift in the criteria used to distinguish between principals (co-perpetrators) and accessories (aiders). The question thus arises as to whether, in the context of ongoing technological advances and the escalating problem of cybercrime, including the use of distributed denial-of-service (DDoS) attacks, the same solution remains applicable. In addition to filling the existing gap in the field, the study employs a novel approach to problem-solving. This involves identifying new problems that have arisen alongside technological advances and attempting to resolve these problems by analysing the paradigmatic solutions.

1. Introduction

Ensuring respect for human rights requires the establishment of clear rules and principles of criminal responsibility, which becomes particularly important with regard to the dual nature of the International Criminal Court (hereinafter: ICC). In fact, the crimes under its jurisdiction are often widespread and systematic, which makes it difficult to establish clear rules that would cover all modes of criminal liability. It is crucial to acknowledge that cybercrimes are exceedingly intricate by nature, and it is a challenging endeavour to differentiate between principals and accessories involved in the crime.

This paper focuses on one type of cybercrime, i.e. *distributed denial-of-service* (hereinafter: DDoS) attacks. This is justified in light of the *CyberPeace Institute* report, which shows that

this type of crime has increased the most since January 2022.[1] It should be noted that the term 'hacking' is used in the text in relation to these attacks, which is not particularly controversial. This is also the terminology used by contemporary authors, as it accurately reflects the process of a DDoS attack.[2] The actual process of DDoS attack begins with the infection of other users with malicious software, for the purpose of creating a so-called *botnet*.[3]

Although the Budapest Convention on Cybercrime[4] and Talinn Manual books[5] have prompted extensive debate on the subject of cyber-operations in an international perspective,[6] it is important to note that this study limits its focus to the issue of cybercrime in the context of the Rome Statute, as acknowledged by the Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare.[7] A number of authors have attempted to reflect on this background by referring, rather generally, to all cybercrimes.[8]

A fairly dominant view in doctrine is that cybercrimes may amount to war crimes under Article 8(2)(b)(i)-(ii), Article 8(2)(b)(iv) and Article 8(2)(e)(i) of the Rome Statute, and although there are also considerations as to whether cybercrimes may also fulfil the element of acts of genocide, crimes against humanity or the crime of aggression, these issues are beyond the scope of this study. A singular view within the doctrine asserts that DDoS actions do not constitute an 'attack' under international humanitarian law.[9] One can also find the view that DDoS attacks are unlikely to fall under the jurisdiction of the International Criminal Court unless they cause serious disruption, property damage or personal injury.[10] These are crucial considerations when examining the wording of Article 8(2)(b)(i)-(ii), Article 8(2)(b)(iv) and

---

[1] CyberPeace Institute, 'Attack Details' <cyberconflicts.cyberpeaceinstitute.org/threats/attack-details> accessed 5 July 2024.

[2] Filip Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym* (1st ed, Wolters Kluwer 2016, Warsaw) 108-112.

[3] The botnet then floods a targeted service with the generated traffic, *ibid*.

[4] *Budapest Convention on Cybercrime*, opened for signature 23 November 2001, ETS No. 185 (entered into force 1 July 2004).

[5] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (1st edn, Cambridge University Press 2013, Cambridge), doi: 10.1017/CBO9781139169288; Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber operations* (2nd edn, Cambridge University Press 2016, Cambridge), doi: 10.1017/9781316822524.

[6] *See, for example,* Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94(886) International Review of the Red Cross 533–578, doi: 10.1017/s1816383113000246; Laurent Gisel, Tilman Rodenhäuser, and Knut Dörmann, 'Twenty years on: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts' (2020) 102(913) International Review of the Red Cross 287–334, doi: 10.1017/s1816383120000387.

[7] Permanent Mission of Liechtenstein to the United Nations, 'Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare' <ila-americanbranch.org/wp-content/uploads/2022/10/The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf> accessed 5 July 2024.

[8] *See, for example*, Oona A. Hathaway, Rebecca Crootof, Philip Levitz *et. al.*, 'The Law of Cyber-Attack' (2012) 100(817) California Law Review 817-886; Kai Ambos, 'International Criminal Responsibility in Cyberspace' in Nicholas Tsagourias, Russell Buchan (eds), *Research Handbook on Cyberspace and International Law* (Edward Elgar Publishing 2015, Cheltenham) 118-143; Marco Roscini, 'Gravity in the Statute of the International Criminal Court and Cyber Conduct that Constitutes, Instigates or Facilitates International Crimes' (2019) 30(3) Criminal Law Forum 247–272, doi: 10.1007/s10609-019-09370-0.

[9] Paul A. Walker, 'Rethinking Computer Network 'Attack': Implications for Law and U.S. Doctrine' (2010) 1(1) Journal of National Security Law & Policy 1-54.

[10] Marco Roscini, 'The International Criminal Court Forum' <iccforum.com/cyberwar> accessed 5 July 2024.

Article 8(2)(e)(i) of the Rome Statute, as each refers to the concept of 'attack' as defined by Article 49 of the Protocol Additional to the Geneva Conventions of 12 August 1949.[11]

Returning to the issue of different modes of criminal liability, it can be argued that the adoption of German legal doctrine by the International Criminal Court represented a significant step forward in addressing challenges to the blurring lines between principals and accessories. It can be said that a kind of consensus as to the criteria for distinguishing between the principal and accessorial forms of crime was reached simultaneously with the judgments of the International Criminal Court in the cases of: *Prosecutor* v. *Thomas Lubanga Dyilo* (hereinafter: Lubanga judgment)[12] and *Prosecutor* v. *Germain Katanga and Mathieu Ngudjolo Chui* (hereinafter: Ngudjolo judgment)[13] This consensus led to the emergence of two related paradigms - the concepts of *funktionelle Tatherrschaft* and *Organisationsherrschaft.*[14] On the one hand, the former paradigm is applied in cases of direct co-perpetration, in which the persons involved exercise functional control over the crime. On the other hand, the latter is used in cases of indirect co-perpetration, i.e. complex criminal activities in which the individuals control the organisation in order to commit the crime.[15] These models are useful for the present research because they have so far been used in international criminal law for the attribution of criminal responsibility in order to define the differences between principal and accessory offenders. The idea behind this paper is for them to continue to be models in solving contemporary problems - such as the aforementioned cybercrime.

To quote the Prosecutor of the International Criminal Court: 'International criminal justice can and must adapt to this new landscape. While no provision of the Rome Statute is dedicated to cybercrimes, such conduct may potentially fulfil the elements of many core international crimes as already defined'.[16] Therefore, the main objective of this article is to integrate the paradigms of international criminal law with the contemporary issue of the evolution of cybercrime. Previous research findings have highlighted the particular significance of conducting a comparative analysis between indirect co-perpetration (*Organisationsherrschaft*) and DDoS-type cyber-attacks.

---

[11] Terry D. Gill, 'International Humanitarian Law Applied to Cyber-Warfare: Precautions, Proportionality, and the Notion of "Attack" Under the Humanitarian Law of Armed Conflict' in Nicholas Tsagourias, Russell Buchan (eds), *Research Handbook on Cyberspace and International Law* (Edward Elgar Publishing 2015, Cheltenham) 366-379.

[12] *Prosecutor* v *Thomas Lubanga Dyilo* (*Judgment*) (International Criminal Court, Trial Chamber I, Case No ICC-01/04-01/06, 14 March 2012).

[13] *Prosecutor* v *Mathieu Ngudjolo Chui* (*Judgment*) (International Criminal Court, Trial Chamber II, Case No ICC-01/04-02/12, 18 December 2012).

[14] Claus Roxin, *Täterschaft und Tatherrschaft* (9th edn, De Gruyter 2015, Berlin).

[15] Jens David Ohlin, Elies Van Sliedregt, Thomas Weigend, 'Assessing the Control-Theory' (2013) 26(3) Leiden Journal of International Law 725-746, doi:10.1017/S0922156513000319; Philipp Osten, 'Indirect Co-Perpetration and the Control Theory: A Japanese Perspective' (2022) 20(3) Journal of International Criminal Justice 677–697, doi: 10.1093/jicj/mqac029.

[16] Karim Asad Ahmad Khan, 'Technology Will Not Exceed Our Humanity' <digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity> accessed 5 July 2024.

2. Theoretical and methodological assumptions

As outlined by Thomas Kuhn, distinct paradigms can coexist within the social sciences. It should be noted, however, that this is not presented as a definitive phenomenon; rather, it is assumed that it can occur.[17] It may therefore be assumed that 'paradigm war' is not a ubiquitous phenomenon in the legal field; indeed, it could be proposed that the occurrence of such a phenomenon is contingent upon a number of factors. It should be noted that the concept of paradigm can be applied not only to broad areas such as the distinction between positivism, post-positivism, interpretivism, but also to narrower issues such as accepted definitions within a particular branch of law. One such example is the decision of the International Criminal Court to reject the joint criminal enterprise doctrine and to adopt the 'control theory'.[18] The adoption of a different theoretical framework has resulted in a shift in the criteria used to distinguish between *principals* (co-perpetrators) and *accessories* (aiders).[19]

It is not necessary to provide a detailed explanation of Kuhn's world-famous assumptions here; instead, it is sufficient to proceed directly to an analysis of international criminal law in the context of these assumptions. It is evident that the mandate of the *ad hoc* tribunals, when the International Criminal Tribunal for the former Yugoslavia and International Criminal Tribunal for Rwanda were consistently applying a subjective theory, can be regarded as a 'normal science' period, during which the judges had paradigm solution to any issue.[20] However, at a certain point, the doctrine began to evolve as a result of numerous objections and criticisms of the representatives of the doctrine against the 'just convict everyone' tendency.[21] The stances of the authors from continental states, where conspiracy legislation was not enacted, played a distinctive role in this 'revolution' process.[22]

It is therefore my view that the period preceding the establishment of the International Criminal Court can be characterised as a period of relative immaturity. The period under discussion is not that of the mandate of the *ad hoc* tribunals, but rather a time when no solution

---

[17] It can be said that there are a number of 'classics' in the field of law that are subject to change, *see* Thomas Kuhn, *The Structure of Scientific Revolutions* (University of Chicago Press 1962, Chicago) 165.

[18] It is commonly asserted that the conviction of Thomas Lubanga Dyilo on 14 March represented a pivotal moment in the history of the ICC. The second significant ruling based on 'control theory' is regarded as that in the Mathieu Ngudjolo Chui case.

[19] For the sake of clarity, I have adopted a certain conceptual framework that is common to the various legal systems, whereby the person who commits the offence is referred to as the principal (direct perpetrator, indirect perpetrator, co-perpetrator) and others, who are not principals, but who participate in committing the offence are referred to as accessories or secondary parties, *see* Michael J. Allen, *Criminal Law* (14th ed, Oxford University Press 2017), p. 241. A similar conceptual framework can also be found in the Hungarian criminal law, which applies dualistic system of the participants (principals/perpetrators and accessories), *see* Balázs Gellér, István Ambrus, *General Principles of Hungarian Criminal Law I* (ELTE Jogi Kari Tankönyvek 2019, Budapest).

[20] The judges adhered to the established findings and reiterated the solutions in cases such as: Prosecutor v Duško Tadić, Prosecutor v Aloys Simba, Prosecutor v Radovan Karadžić, Prosecutor v Elizaphan Ntakirutimana and Gérard Ntakirutimana, Prosecutor v Radoslav Brđanin. On the concept of 'normal science period', see Kuhn (n 17) 23-35.

[21] For further information regarding the third type of joint criminal enterprise and the issues associated with it, *see* Mohamed Elewa Badar, 'Just Convict Everyone! – Joint Perpetration: From Tadić to Stakić and Back Again' 2006 6(2) International Criminal Law Review 293-302, doi: 10.1163/157181206778050679.

[22] Representatives of the continental states, including German authors such as Kai Ambos, have played a key role here. For example, to learn about the author's postulates, *see* Kai Ambos, 'Joint Criminal Enterprise and Command Responsibility' 2007 5(1) Journal of International Criminal Justice 159-183, doi: 10.1093/jicj/mql045.

had been reached to the question of the criterion between principals and accessories in international criminal law. During that period, a multiplicity of authors engaged in discourse around different and competing theoretical frameworks, resulting in a lack of common progress. It was only after the judgments in the Lubanga and Ngudjolo cases that new paradigms began to emerge, offering potential solutions within the mature scientific community.

> But paradigms […] are the source of the methods, problem-field, and standards of solution accepted by any mature scientific community at any given time. As a result, the reception of a new paradigm often necessitates a redefinition of the corresponding science.[23]

The subjective theory of the joint criminal enterprise doctrine used by *ad hoc* tribunals distinguished between an aider and a principal perpetrator on the basis of the joint intent.[24] The German theory, however, considers the question of the exercise of control over the criminal act to be a demarcation criterion.[25] In the absence of such 'control' element, the individual in question is classified as an accessory. Although there is no absolute distinction between the categories under consideration in terms of their classification as either true (*science*) or false (*non-science*), the definitions provided for each category are in fact mutually exclusive. Without delving further into the issues of legal philosophy, the aforementioned sentence touches upon other theses that acknowledge the importance of seeking logical coherence rather than truth and falsity in legal matters.[26]

From the above, it can be seen that the theoretical method has been applied to understand the complex issues of international criminal law. In addition, the doctrinal research method has been used to achieve the outlined research objective. It should be noted that the research tasks within this study have been aimed at analysing material from sources of international criminal law, case law and literature. The sources of international criminal law can be broadly categorised as follows: international treaties, general principles of international criminal law, resolutions of international bodies and subsidiary means of determining the law. In summary, the present study is mainly based on *black-letter research*, which takes the form of qualitative research in the selection and weighing of materials, taking into account social context and interpretation.[27]

---

[23] Kuhn (n 17) 103.

[24] *See, for example,* Giulia Bigi, 'Joint Criminal Enterprise in the Jurisprudence of the International Criminal Tribunal for the Former Yugoslavia and the Prosecution of Senior Political and Military Leaders: The Krajišnik Case' 2010 14(1) Max Planck Yearbook of United Nations Law Online 51-83, doi: 10.1163/18757413-90000049.

[25] Roxin (n 14).

[26] It is necessary to distinguish between the truth of the statement and the problem of its correct construction in terms of logical syntax. On Wittgenstein I, von Wright's postulates, and the views of many other authors, *see* Marek Zirk-Sadowski, *Wprowadzenie do filozofii prawa* (1st edn, Wolters Kluwer 2011, Warsaw) 82-93.

[27] Ian Dobinson, Johns Francis, 'Qualitative Legal Research' in Mike McConville and Wing Hong Chui (eds), *Research Methods for Law* (Edinburgh University Press 2007, Edinburgh 16-41), 21.

3. Cybercrime from the perspective of the control-over-the-crime theory

3.1. DDoS attack - an analysed cybercrime

Prior to undertaking a jurisdictional analysis, it is essential to provide a brief description of what constitutes a DDoS attack. It could be stated that a DDoS attack is a cybercrime that aims to impede the functionality of an infrastructure by generating a substantial volume of traffic.[28] It is crucial to emphasise that this paper focuses on an advanced variant of denial-of-service attacks, characterised by the usage of botnets i.e., networks of intermediary other users' computers. The attack initiates with the hacker installing malware programmes, which remain 'dormant' until activated by the hackers. At a pre-determined point in time, a surge of data is transmitted to the targeted infrastructure via the devices of unsuspecting users, without their consent or awareness.

While this may appear to be a relatively minor issue, it is, in fact, a significant one. A case study of a real-world incident can be found from 2014, when Boston Children's Hospital was subjected to DDoS attack by the hacking collective known as Anonymous. Without commenting on the motives of this group, the attack had the potential to bring down multiple parts of Boston's critical healthcare infrastructure due to the hospital's use of the same Internet Service Provider as seven other healthcare institutions in the area. As indicated in the Radware's report, the contemporary global situation has reached a point where cyber-attacks have the potential to be 'more than merely disruptive and expensive; they can also be deadly'.[29] The judgment in the case against the identified perpetrator, Martin Gottesfeld, provides further evidence that DDoS attacks can have significant consequences, with the court defining them as 'serious and undoubtedly creating a substantial risk of significant harm to many persons, especially patients'.[30] It seems reasonable to conclude that this type of act should be linked to serious crimes, particularly given that the perpetrator in the above case was sentenced to 10 years in prison.[31]

This paper does not deal with attacks by private hackers operating on a small scale. Rather, the focus of this paper is on those attacks that have the potential to fall under the jurisdiction of the International Criminal Court. The Russian forces are already targeting Ukrainian children's hospitals with missile strikes.[32] While launching missiles is undoubtedly a war crime, this

[28] Radoniewicz (n 2).

[29] Radware's Threat Alert, 'DDoS Case Study: Boston Children's Hospital DDoS Attack Mitigation' (2015) <radware.com/security/ddos-experts-insider/ert-case-studies/boston-childrens-hospital-ddos-mitigation-case-study> accessed 5 July 2024. *See also* quoted in Radware's Report, Daniel J. Nigrin, 'When Hacktivists Target Your Hospital' (2014) 371(5) New England Journal of Medicine, doi: 10.1056/NEJMp1407326.

[30] *United States* v *Gottesfeld* (*Judgment*) (United States Court of Appeals, First Circuit, Case No 18 F.4th 1, 5 November 2021).

[31] An additional argument for considering that it is a 'serious crime' is the definition proposed by the Palermo Convention, which defines serious crime as conduct that constitutes an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty. In the case of Polish legislation, for example, the interference with a computer system is punishable by up to five years' imprisonment.

[32] Svitlana Vlasova, Daria Tarasova-Markina, Maria Kostenko, Victoria Butenko and Lauren Said-Moorhouse, 'Ukrainian children's hospital attacked as Russian strikes on cities kill at least 43' (2024)

article adds to the argument that attacks on hospitals from cyberspace are more silent, 'behind the scenes', and should not be left out of the picture.[33] This is not the first time that the importance of focusing attention on the issue of pro-Russian cyber activity has been emphasised in the context of the war in Ukraine.[34] If a number of arrest warrants have already been issued with regard to Russian perpetrators, the cyber-related crimes should also be considered.[35]

Furthermore, this approach would not be incompatible with the principle of *nullum crimen sine lege*.[36] In order to consider the implications of DDoS attacks, it would be necessary to examine those provisions that provide for the intentional targeting of the population or civilian objects. The concept of 'attack' is not limited to kinetic means in Article 8(2)(b)(i), (ii) and (iv) of the Rome Statute; rather it encompasses all cyber operations that result in physical damage to persons or damage to objects beyond the attacked computer program or data.[37] In fact, the defining characteristic of an attack under international humanitarian law is not the severity of the employed means, but rather the severity of the resulting consequences, even if they are indirect.[38] Consequently, in my view, if a DDoS attack results in the deaths of patients in a hospital, this constitutes a war crime, regardless of whether the attack was initiated through a cyber-attack or through the use of missile rockets.

The criterion of 'gravity' should be considered from two perspectives. Firstly, it is necessary to determine whether the individuals likely to be the subject of investigation or prosecution include those 'most responsible' for the alleged crimes. Secondly, it is essential to assess the quantitative and qualitative factors involved, including the nature, scale, manner of commission and impact of the alleged crimes.[39] The admissibility of DDoS attacks directed by Russian hacking groups under Article 17(d) of the Rome Statute would depend on several factors, including whether the individuals deemed 'most responsible' were investigated, the extent of injury or material damage caused by the attack (*scale*), and whether the attack resulted in the death of Ukrainian victims (*nature*). It is beyond doubt that the context of the over two-year systematic Russian invasion of Ukraine would have constituted an aggravating factor (*manner of commission*). Furthermore, in addition to the devastating impact on the victims, the attack would have added another factor to the already prevailing disapproval of Russian policy within the international community (*impact*).

<edition.cnn.com/2024/07/08/europe/ukraine-russian-strike-childrens-hospital-intl/index.html> accessed 5 July 2024.

[33] On the need to consider 'invisible atrocities', *see* Randle C. DeFalco, *Invisible Atrocities: The Aesthetic Biases of International Criminal Justice* (Cambridge University Press 2022, Cambridge) 250.

[34] See, for example, Healthcare IT News, 'Shields up' say feds in response to potential Russian escalation' (2022) <healthcareitnews.com/news/shields-say-feds-response-potential-russian-escalation> accessed 5 July 2024; Cybersecurity Advisory, Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (2022) <cisa.gov/news-events/cybersecurity-advisories/aa22-110a> accessed 5 July 2024.

[35] With regard to the situation in Ukraine, the ICC judges have already issued arrest warrants against: Vladimir Vladimirovich Putin and Maria Alekseyevna Lvova-Belova; Sergei Ivanovich Kobylash and Viktor Nikolayevich Sokolov; Sergei Kuzhugetovich Shoigu and Valery Vasilyevich Gerasimov.

[36] For discussion on principles *nullum crimen sine lege* and *nulla poena sine lege*, *see* Balázs József *Gellér, Nemzetközi Büntetőjog Magyarországon. Adalékok egy vitához (Tullius Kiadó 2009, Budapest) 45.*

[37] Knut Dörmann*,* 'Part II. Analysis and Interpretation of Elements: Article 8. War crimes' in Otto Triffterer, Kai Ambos (eds), *Rome Statute of the International Criminal Court: A Commentary* (3rd edn, C.H. Beck 2016, Monachium, 295-580) 355.

[38] *Ibid.*

[39] Roscini (n 8) 255.

3.2. DDoS attacks from the perspective of the further developed model of control-over-the crime theory (Organisationsherrschaft)

In light of the aforementioned considerations, it is necessary to consider the subsequent steps that should be taken. In the event that the Court determines that the case is admissible and falls within the jurisdiction of the International Criminal Court, what would be the appropriate course of action? This research aims to provide a preliminary answer to this question. It suggests that the most suitable approach would be to frame this cybercrime within the framework that the Court has already employed, namely *Organisationsherrschaft.* This concept is derived from 'control theory' and has been applied in a number of cases, including the Ngudjolo judgment.

It can be posited that indirect co-perpetration, which involves the 'control of an organisation', is a combination of indirect perpetration and co-perpetration. Perpetrator A, who exercises vertical control over the militia carrying out their orders, and also engages in horizontal cooperation with another perpetrator, B, is regarded as an indirect co-perpetrator.[40] In accordance with the Roxin's theoretical framework, three key elements are identified on these grounds: the existence of a hierarchical structure with a vertical configuration (*the apparatus of power*), the unlimited exchangeability of the direct actor (*fungibility*), and the operation of the apparatus outside the legal order (*detachment from the law*).[41]

In this context, the term *Hintermann* refers to the domination of the hackers over the users connected to the botnet. Those users connected to the botnet (*Frontmann*) lack the requisite intent to commit a crime, and thus exhibit a deficit in this regard.[42] It could be stated that the botnet is created from users who are interchangeable, and the refusal of any of them to commit an act (e.g. realising that a device is infected and stopping to take part in a flooding attack) cannot negatively affect the implementation of the criminal hacking plan (*fungibility*). One could cautiously say that the botnet organisation is detached from the legal order, bearing in mind that this criterion has been questioned by Kai Ambos, who argues that while it may exist, it is not an inherent condition when considering the *Organisationsherrschaft* concept.[43]

---

[40] Jens David Ohlin, 'Second-Order Linking Principles: Combining Vertical and Horizontal Modes of Liability' 2012 25(3) Leiden Journal of International Law 771-797, 778, doi:10.1017/S0922156512000386.

[41] For more recent studies in English, which include the theses of Claus Roxin and Henning Radtke, see Johannes Block, *Reconciling Responsibility with Reality: A Comparative Analysis of Modes of Active Leadership Liability in International Criminal Law* (1st edn, T.M.C. Asser Press 2023, The Hague 2023), doi: 10.1007/978-94-6265-607-9.

[42] Neha Jain, 'The Control Theory of Perpetration in International Criminal Law' (2011) 12(1) Chicago Journal of International Law 157-198, 169.

[43] Kai Ambos, 'Tatherrschaft durch Willensherrschaft kraft organisatorischer Machtapparate' (1998) 145 Goltdammer's Archiv für Strafrecht 226-245, 243.

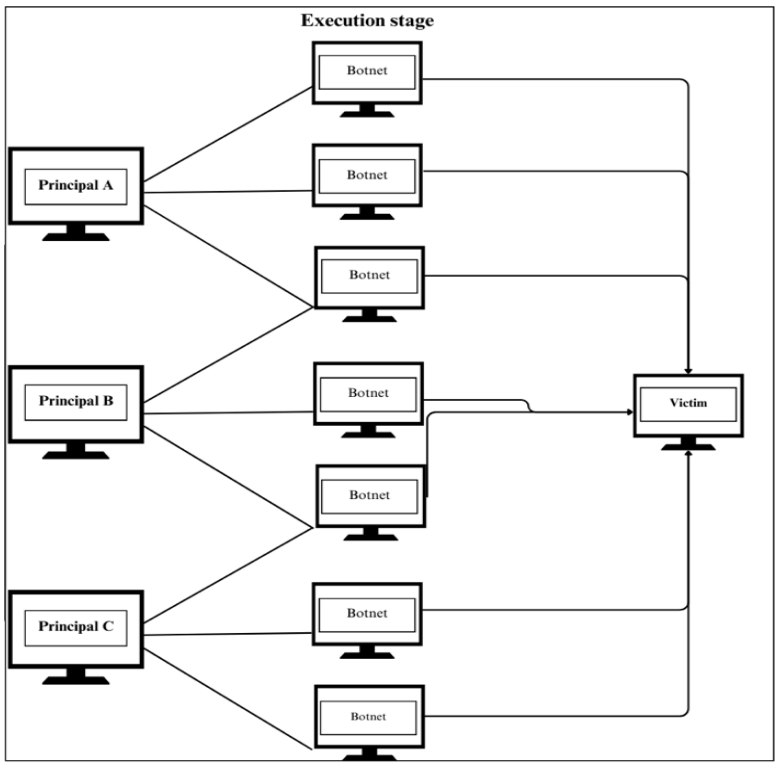

Figure I. Simplified illustration of the *DDoS* attacks.

The above conclusions can be seen in ***Figure I***. As explained earlier, a botnet is defined as a group of devices under the control of malicious actors, referred to in ***Figure I*** as Principal A, Principal B and Principal C. The malware runs silently in the background of the computers, meaning that users of infected computers are used as 'tools'. Principals A, B and C are responsible for the crimes committed by virtue of their control over the entire network, exercised through the use of intermediaries whose devices are part of the botnet.

There is not enough space in this paper for me to detail all the modifications that need to be made to the concept of 'control over the organisation' (*Organisationsherrschaft*) to make it fully applicable to DDoS cybercrime. Nevertheless, these adjustments do not represent a fundamental shift in the underlying paradigm. It is my view that the paradigm remains applicable, provided that the requisite modifications are implemented. While the aspect of fungibility, in the context of the interchangeability of users, is met, the requirement of 'detachedness from the legal order' needs to be considered, as well as the definition of 'hierarchical, vertically structured organisation'. Can this definition be extended to a botnet, given that it generates almost automatic compliance? This is undoubtedly a question I would like to explore further in my future research.

4. Conclusions

In conclusion, it has been preliminarily established that cybercrimes involving DDoS attacks committed during the period of a conflict of an international nature may fall within the ICC's jurisdiction. With regard to the second part of this study, it has been preliminarily concluded

that indirect co-perpetration, based on the control-over-the-crime theory, is well-suited to the specifics of DDoS attacks; however, a clarification of the definition 'organisation' is required.

It is evident that elaborating on DDoS attacks solely from the general international public law point of view is insufficient,[44] in particularly in light of the widespread acts committed by organised pro-Russian hacker groups. In order to establish a clear framework for understanding the actions of these groups and the criminal liability associated with them, there is a pressing need for the development of clear principles and definitions pertaining to the various modes of liability**.** Apart from the fact that the issues addressed are not widely discussed on the grounds of international criminal law, there is a dearth of studies in doctrine that examine this issue in more detail from the perspective of the *fair labelling principle*.[45]

Literature

Allen, M. J., *Criminal Law* (14th ed, Oxford University Press 2017). DOI: https://doi.org/10.1093/he/9780198788676.001.0001

Ambos, K., 'International Criminal Responsibility in Cyberspace' in Nicholas Tsagourias, Russell Buchan (eds), *Research Handbook on Cyberspace and International Law* (Edward Elgar Publishing 2015, Cheltenham) 118-143. DOI: https://doi.org/10.4337/9781782547396.00015

Ambos, K., 'Joint Criminal Enterprise and Command Responsibility' 2007 5(1) Journal of International Criminal Justice 159-183, DOI: https://doi.org/10.1093/jicj/mql045.

Ambos, K., 'Tatherrschaft durch Willensherrschaft kraft organisatorischer Machtapparate' (1998) 145 Goltdammer's Archiv für Strafrecht 226-245, 243.

Badar, M.E., 'Just Convict Everyone! – Joint Perpetration: From Tadić to Stakić and Back Again' 2006 6(2) International Criminal Law Review 293-302, DOI: https://doi.org/10.1163/157181206778050679.

Bigi, G., 'Joint Criminal Enterprise in the Jurisprudence of the International Criminal Tribunal for the Former Yugoslavia and the Prosecution of Senior Political and Military Leaders: The Krajišnik Case' 2010 14(1) Max Planck Yearbook of United Nations Law Online 51-83, DOI: https://doi.org/10.1163/18757413-90000049.

Block, J., *Reconciling Responsibility with Reality: A Comparative Analysis of Modes of Active Leadership Liability in International Criminal Law* (1st edn, T.M.C. Asser Press 2023, The Hague 2023), DOI: https://doi.org/10.1007/978-94-6265-607-9.

[44] *Cf.* Stefan Kirchner, 'Distributed Denial-of-Service Attacks under Public International Law: State Responsibility in Cyberwar' 2009 8(3) The IUP Journal of Cyber Law 10-23.

[45] James Chalmers, Fiona Leverick, 'Fair Labelling in Criminal Law' 2008 71(2) Modern Law Review 217-246, doi: 10.1111/j.1468-2230.2008.00689; Douglas Guilfoyle, 'Responsibility for Collective Atrocities: Fair Labelling and Approaches to Commission in International Criminal Law' 2011 64(1) Current Legal Problems 255-286, doi: 10.1093/clp/cur006.

Chalmers, J., Leverick, F., 'Fair Labelling in Criminal Law' 2008 71(2) Modern Law Review 217-246, DOI: https://doi.org/10.1111/j.1468-2230.2008.00689.x.

Dobinson, I., Francis, J., 'Qualitative Legal Research' in Mike McConville and Wing Hong Chui (eds), Research Methods for Law (Edinburgh University Press 2007, Edinburgh 16-41).

Droege, C., 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94(886) International Review of the Red Cross 533–578, DOI: https://doi.org/10.1017/S1816383113000246.

Gellér, B., Ambrus, I., *General Principles of Hungarian Criminal Law I* (ELTE Jogi Kari Tankönyvek 2019, Budapest).

Gellér, B.J., *Nemzetközi Büntetőjog Magyarországon. Adalékok egy vitához* (Tullius Kiadó 2009, Budapest).

Gill, T.D., 'International Humanitarian Law Applied to Cyber-Warfare: Precautions, Proportionality, and the Notion of "Attack" Under the Humanitarian Law of Armed Conflict' in Nicholas Tsagourias, Russell Buchan (eds), *Research Handbook on Cyberspace and International Law* (Edward Elgar Publishing 2015, Cheltenham) 366-379. DOI: https://doi.org/10.4337/9781782547396.00029.

Gisel, L., Rodenhäuser, T., and Dörmann, K., 'Twenty years on: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts' (2020) 102(913) International Review of the Red Cross 287–334, DOI: https://doi.org/10.1017/S1816383120000387.

Guilfoyle, D., 'Responsibility for Collective Atrocities: Fair Labelling and Approaches to Commission in International Criminal Law' 2011 64(1) Current Legal Problems 255-286, DOI: https://doi.org/10.1093/clp/cur006.

Hathaway, O.A., Crootof, R., Levitz P. *et. al.*, 'The Law of Cyber-Attack' (2012) 100(817) California Law Review 817-886.

Jain, N., 'The Control Theory of Perpetration in International Criminal Law' (2011) 12(1) Chicago Journal of International Law 157-198, 169.

Kirchner, S., 'Distributed Denial-of-Service Attacks under Public International Law: State Responsibility in Cyberwar' 2009 8(3) The IUP Journal of Cyber Law 10-23.

Knut Dörmann, 'Part II. Analysis and Interpretation of Elements: Article 8. War crimes' in Otto Triffterer, Kai Ambos (eds), *Rome Statute of the International Criminal Court: A Commentary* (3rd edn, C.H. Beck 2016, Monachium, 295-580).

Kuhn, T., *The Structure of Scientific Revolutions* (University of Chicago Press 1962, Chicago) 165.

Nigrin, D.J., 'When Hacktivists Target Your Hospital' (2014) 371(5) New England Journal of Medicine, DOI: https://doi.org/10.1056/NEJMp1407326.

Ohlin, J.D., 'Second-Order Linking Principles: Combining Vertical and Horizontal Modes of Liability' 2012 25(3) Leiden Journal of International Law 771-797, 778, DOI: https://doi.org/10.1017/S0922156512000386.

Ohlin, J.D., Van Sliedregt, E., Weigend, T., 'Assessing the Control-Theory' (2013) 26(3) Leiden Journal of International Law 725-746, DOI: https://doi.org/10.1017/S0922156513000319.

Osten, P., 'Indirect Co-Perpetration and the Control Theory: A Japanese Perspective' (2022) 20(3) Journal of International Criminal Justice 677–697, DOI: https://doi.org/10.1093/jicj/mqac029.

Radoniewicz, F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym* (1st ed, Wolters Kluwer 2016, Warsaw).

Randle C. DeFalco, *Invisible Atrocities: The Aesthetic Biases of International Criminal Justice* (Cambridge University Press 2022, Cambridge). DOI: https://doi.org/10.1017/9781108766692.

Roscini, M., 'Gravity in the Statute of the International Criminal Court and Cyber Conduct that Constitutes, Instigates or Facilitates International Crimes' (2019) 30(3) Criminal Law Forum 247–272, DOI: https://doi.org/10.1007/s10609-019-09370-0.

Roxin, C., *Täterschaft und Tatherrschaft* (9th edn, De Gruyter 2015, Berlin). DOI: https://doi.org/10.1515/9783110366594.

Schmitt, M.N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber operations* (2nd edn, Cambridge University Press 2016, Cambridge), DOI: https://doi.org/10.1017/9781316822524.

Schmitt, M.N., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (1st edn, Cambridge University Press 2013, Cambridge), DOI: https://doi.org/10.1017/CBO9781139169288.

Walker, P.A., 'Rethinking Computer Network 'Attack': Implications for Law and U.S. Doctrine' (2010) 1(1) Journal of National Security Law & Policy 1-54.

Zirk-Sadowski, M., *Wprowadzenie do filozofii prawa* (1st edn, Wolters Kluwer 2011, Warsaw).

Cases

Prosecutor v *Mathieu Ngudjolo Chui* (*Judgment*) (International Criminal Court, Trial Chamber II, Case No ICC-01/04-02/12, 18 December 2012).

Prosecutor v *Thomas Lubanga Dyilo* (*Judgment*) (International Criminal Court, Trial Chamber I, Case No ICC-01/04-01/06, 14 March 2012).

United States v *Gottesfeld* (*Judgment*) (United States Court of Appeals, First Circuit, Case No 18 F.4th 1, 5 November 2021).

Other sources

Budapest Convention on Cybercrime, opened for signature 23 November 2001, ETS No. 185 (entered into force 1 July 2004).

CyberPeace Institute, 'Attack Details' <cyberconflicts.cyberpeaceinstitute.org/threats/attack-details> accessed 5 July 2024.

Cybersecurity Advisory, Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (2022) <cisa.gov/news-events/cybersecurity-advisories/aa22-110a> accessed 5 July 2024.

Healthcare IT News, 'Shields up' say feds in response to potential Russian escalation' (2022) <healthcareitnews.com/news/shields-say-feds-response-potential-russian-escalation> accessed 5 July 2024.

Khan, K.A.A., 'Technology Will Not Exceed Our Humanity' <digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity> accessed 5 July 2024.

Permanent Mission of Liechtenstein to the United Nations, 'Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare' <ila-americanbranch.org/wp-content/uploads/2022/10/The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf> accessed 5 July 2024.

Radware's Threat Alert, 'DDoS Case Study: Boston Children's Hospital DDoS Attack Mitigation' (2015) <radware.com/security/ddos-experts-insider/ert-case-studies/boston-childrens-hospital-ddos-mitigation-case-study> accessed 5 July 2024.

Roscini, M. 'The International Criminal Court Forum' <iccforum.com/cyberwar> accessed 5 July 2024.

Svitlana Vlasova, Daria Tarasova-Markina, Maria Kostenko, Victoria Butenko and Lauren Said-Moorhouse, 'Ukrainian children's hospital attacked as Russian strikes on cities kill at least 43' (2024) <edition.cnn.com/2024/07/08/europe/ukraine-russian-strike-childrens-hospital-intl/index.html> accessed 5 July 2024.