Bálint-Imre Bodó*

Cybersecurity and International Criminal Law

Abstract

In this paper I thoroughly discuss the possibility of committing crimes which would fall under the Rome Statute, with regards to the very notion of cybersecurity. I conclude that we need extensively empirical research and solution to many aspects pointed out in my paper. First, we need to find an acceptable definition of cybersecurity to work with this process, and in order to understand the world and possibilities it creates for us. Furthermore, the 1998 Rome Statute needs an update, because the world of the internet creates opportunities never seen before, and the international case law is unable to cope with such distinct acts. Therefore, I believe that we need to find the next „Nuremberg Trials", the next generational solution to a world and crimes never seen before. We need the theoretical and legal revolution which did come after the World World II, and after the ICTY, ICTR and Sierra Leone ad hoc Courts. I truly hope that this short and hence mashup summarizing paper is just an indicator of papers and conferences to come, with solutions and more and more ideas on how we solve these two phased problems, namely having to find 1. An ultimate definition for cybersecurity 2. Having a solution of how to interpret it to the classical notion of International Criminal Law. if we conclude that we are unable to handle this issue, I suggest to create a panel on international or V4 level on either the reorganization of customary international criminal law under the Rome Statute or on the ever-changing definition of cybersecurity.

Key words: Cybersecurity, Criminal Law, International Law, International Criminal Law, Genocide, Other Inhuman Acts

* Bálint-Imre Bodó, MA Student at the Eötvös Loránd University Faculty of Law, e-mail: bodo.balint98@gmail.com.

Introduction

„Order is necessary and chaos inimical to a just and stable existence"[1]. In 2013 the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) determined that the application of norms derived from existing international law is to minimize risks to world peace and international security and stability[2].

The ubiquity of the technology underlying the Internet[3], which is not restricted by national borders, renders strictly single-state regulation largely ineffective. International law is needed to ensure cybersecurity legitimately and effectively in the common interest of all states. This is not a new insight[4]. Without legitimate and effective protection of cybersecurity under international law, individuals and societies cannot develop to their full potential.

International Criminal Law as a subsequent field of International Law has the aim of ensuring the very protection of individuals by punishing the harshest crimes. This field of law adopts a combination of the classic common law and historical evolution of international criminal law.

In this paper I will discuss the legal definition of the so-called core crimes – war crimes, crimes against humanity, genocide – plus aggression, torture and terrorism and try to ascertain whether the criminal action could be adopted or modified or even applied to the definition – if such exists – of cybersecurity. I will try to describe the forms and modes of criminal responsibility when it would come to cybersecurity and assess if a cybersecure action is being done would such action be enough to conclude or initiate the international criminal responsibility; and the main issues related to the prosecution and punishment of international crimes at the national and international level, including amnesties, statutes of limitations and immunities.

1 M.N. Shaw, *International Law*, ed. 6, Oxford 2008, p. 1.

2 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, June 24, 2013, para. 16.

3 M.N. Schmitt, L. Vihul, *The Nature of International Law Cyber Norms*, „Tallinn Paper" 2014, no. 5, p. 16; K. Ziolkowski, *General Principles of International Law as Applicable in Cyberspace* [in:] *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, ed. idem, Tallinn 2013, p. 135–184, 151–152.

4 UN General Assembly Resolution 53/70, Developments in the field of information and telecommunications in the context of international security, A/RES/53/70, of January 4, 1999, para. 2c, http://www.un.org/ga/search/view-doc.asp?symbol=AIRES/53/70 [access: 20.01.2022].

The extremely Brief History of International Criminal Law

The International Criminal Law started off with the Nuremberg Trials (hereinafter: IMT = International Military Tribunal at Nuremberg)[5]. The IMT trial was the first international criminal trial and, to this day, it remains the most prominent. The „trial of the century" was convened in the aftermath of the collapse of the Third Reich, the destruction caused by World War II, and the horror of the unparalleled atrocities committed by the Axis Powers. Retribution for these crimes was declared as one of the principal Allied war aims as early as 1941, and by 1943, the Allies had decided to set up a commission to gather evidence of Nazi crimes. In August 1945, the four Allied Powers of France, the Soviet Union, the United Kingdom and the United States (the „Four Powers") signed the London Agreement, paving the way for the prosecution of major war criminals before the IMT.

It must be common knowledge by now, at least among international lawyers, that it was the fateful decision of the UN Security Council to establish the International Criminal Tribunal for the former Yugoslavia (ICTY) in 1993[6] and the International Criminal Tribunal for Rwanda (ICTR) in 1994[7]. To prosecute atrocity crimes in the Balkans and East Africa that rescued the idea of international criminal law (ICL). The SCSL, whose work began in 2002 and concluded in 2013, followed in the footsteps of the ICTY and the ICTR. The SCSL benefited from its predecessors but also introduced a new „hybrid" model of the international criminal tribunal.

An ad hoc model that, for various reasons including its mixed subject matter jurisdiction and local ownership, has proved to be of relevance for States as a means of providing credible justice for international crimes, despite the initial impression that the creation of a permanent International Criminal Court (ICC) would render them superfluous[8].

At the heart of this justice discourse was a legacy and set of sentimental commitments against mass atrocity violence that is said to have continued from various twentieth-century trials, including the Nuremberg tribunal of

5 Nuremberg Trial Archives The International Court of Justice: custodian of the archives of the International Military Tribunal at Nuremberg.
6 S.C. Res. 827 (May 25, 1993).
7 S.C. Res. 955 (Nov. 8, 1994).
8 Rome Statute of the International Criminal Court, July 1, 2002, 2187 U.N.T.S. 3.

the late 1940s. On July 17, 1998, led 120 of the world's leaders to sign the Rome Statute to establish the International Criminal Court.

The insistence that various publics, constituting the international community, have a responsibility to protect those victimized by such violence. Also central to it is a vehemently articulated anti-impunity discourse that insists that no one (high-ranking leaders, politicians, presidents, rebels, or ordinary citizens) should be beyond the reach of the law.

The ICC anti-impunity narrative insists not only that justice means individual perpetrators should be punished, but that a perpetrator's official capacity should not bar him or her from criminal investigation. Understanding justice not solely in relation to the visible application of the law at all costs, but also as negotiated assemblages of feelings about inequality and power; allowing us to reflect on the biggest changes in the world – namely crimes throughout the internet.

The main principle did not change during our years, since any person who commits an act which constitutes a crime under international law is responsible therefor and liable to punishment.

In this paper, I will only refer to the instrument and cases of the ICC, for better understanding I refer to previous writings[9].

The Applicable International Criminal Core Law in relation with Cybersecurity

In my opinion there are two main characteristic crimes which could be applied to the notion of cybersecurity, in terms of international criminal law; naturally in normal times – thus excluding war crimes as such.

According to the United Nations (hereinafter: UN) 1998 Rome Statute[10] Art. 6 (c) Genocide is the act in which by deliberately inflicting conditions of life calculated to bring about physical destruction. The Elements needed to be fulfilled are the following: 1. The perpetrator inflicted certain conditions of life

9 See as an example: K. Heller, *The Rome Statute of the International Criminal Court* [in:] *The Handbook of Comparative Criminal Law*, eds. idem, M. Dubber, Redwood City 2010, p. 593–634.

10 Done at Rome on 17 July 1998, in force on 1 July 2002, United Nations, Treaty Series, vol. 2187, no. 38544, Depositary: Secretary-General of the United Nations, http://treaties.un.org [access: 20.01.2022].

upon one or more persons. 2. Such person or persons belonged to a particular national, ethnical, racial, or religious group. 3. The perpetrator intended to destroy, in whole or in part, that national, ethnical, racial, or religious group, as such. 4. The conditions of life were calculated to bring about the physical destruction of that group, in whole or in part. The conduct took place in the context of a manifest pattern of similar conduct directed against that group or was conduct that could itself effect such destruction.

We have to assess the „crime against humanity", which means any of the following acts when committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack: (not full closured list, I will just highlight the most important ones) (a) Murder; (k) Other inhumane acts of a similar character intentionally causing great suffering, or serious injury to body or to mental or physical health.

Since Art. 7 pertains to international criminal law, its provisions, consistent with Art. 22, must be strictly construed, taking into account that crimes against humanity as defined in art. 7 are among the most serious crimes of concern to the international community as a whole, warrant and entail individual criminal responsibility, and require conduct which is impermissible under generally applicable international law, as recognized by the principal legal systems of the world. The elements clarify the requisite participation in and knowledge of a widespread or systematic attack against a civilian population. However, the last element should not be interpreted as requiring proof that the perpetrator had knowledge of all characteristics of the attack or the precise details of the plan or policy of the State or organization. In the case of an emerging widespread or systematic attack against a civilian population, the intent clause of the last element indicates that this mental element is satisfied if the perpetrator intended to further such an attack.

To the ends of torture 1. the perpetrator must have inflicted severe physical or mental pain or suffering upon one or more persons. 2. Such person or persons were in the custody or under the control of the perpetrator. 3. Such pain or suffering did not arise only from, and was not inherent in or incidental to, lawful sanctions. 4. The conduct was committed as part of a widespread or systematic attack directed against a civilian population. 5. The perpetrator knew that the conduct was part of or intended the conduct to be part of a widespread or systematic attack directed against a civilian population.

In terms of „other inhumane acts":

1. The perpetrator inflicted great suffering, or serious injury to body or to mental or physical health, by means of an inhumane act.

2. Such act was of a character similar to any other act referred to in art. 7, para. 1, of the Statute.

3. The perpetrator was aware of the factual circumstances that established the character of the act.

4. The conduct was committed as part of a widespread or systematic attack directed against a civilian population.

5. The perpetrator knew that the conduct was part of or intended the conduct to be part of a widespread or systematic attack directed against a civilian population.

Definition of cybersecurity

When speaking about international criminal law, we always must understand the underlying act, in our case this understanding cannot be done without the deep knowledge about the definition of cybersecurity. Indeed, cybersecurity as such is not aa form of conduct to an act, nor is it an omission, but without understanding it we find ourselves in the middle of nowhere. „A science of cybersecurity offers many opportunities for advances based on a multidisciplinary approach, because, after all, cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines. So, in addition to the critical traditional fields of computer science, electrical engineering, and mathematics, perspectives from other fields are needed”[11].

In this short subsequent part, I will try to demonstrate the definitions of cybersecurity in literature. Naturally when reading this paper one must ask, how does it come that there are more and more definitions in use. This is due firstly to the reason that our legal systems function so differently, there are countries – like Hungary and Poland – who are truly working on coming up with solutions, and there are totally different common law countries in which just by the definition of law something is understood differently. Secondly cybersecurity is such a broad concept that a general definition is almost impossible to give, therefore after listing some of the key definitions from the literature I will demonstrate the definition with which I am working later. Thirdly, cybersecurity is a moving term, not because we from the point of view

11 F.R Chang, *Guest Editor's Column*, „The Next Wave” 2012, vol. 19, no. 4, p. 1–2.

of science would want it, but the underlying circumstances change so quickly that we must come up with new and more new solutions in order to follow it.

As mentioned above cybersecurity is a broadly used term, whose definitions are highly variable, often subjective, and at times, uninformative. The absence of a concise, broadly acceptable definition that captures the multidimensionality of cybersecurity impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges.

Among the possible information sources, we might expect legislators facing uncertainty over problem definition and who has authority to regulate emerging, disruptive technologies to turn to federal bureau-crats in particular; bureaucracies represent institutionalized problem definitions, and the bureaucrats themselves are sources of expertise about both issue substance and the regulatory process[12].

„Cyber" is a prefix connoting cyberspace and refers to electronic communication networks and virtual reality according to the Oxford Dictionary. Once's coming to the definitions this paper enlists the following ones: 1) Public Safety Canada (2010) defines cyberspace as "the electronic world created by interconnected networks of information technology and the information on those networks. It is a global common where people are linked together to exchange ideas, services and friendship"[13]; 2) „Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders"[14]; 3) „Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption"[15]; 4) „Cyber Security involves reducing the risk of malicious attack to software, computers and networks. This includes tools used to detect break-ins, stop viruses, block malicious access,

12 S. Workman, *The Dynamics of Bureaucracy in the U.S. Government: How Congress and Federal Agencies Process Information and Solve Problems*, New York 2015; S. Workman, J. Shafran, T. Bark, *Problem Definition and Information Provision by Federal Bureaucrats*, „Cognitive Systems Research" 2017, vol. 43, p. 140–152.

13 *Canada's Cyber Security Strategy*, Ottawa 2010.

14 R.A. Kemmerer, *Cybersecurity* [in:] *Proceedings of the 25th IEEE International Conference on Software Engineering, 2003*, p. 705–715, http://dx.doi.org/10.1109/ICSE.2003.1201257 [access: 25.01.2022].

15 J.A. Lewis, *Cybersecurity and Critical Infrastructure Protection*, Washington, DC 2006.

enforce authentication, enable encrypted communications, and on and on"[16]; 5) „Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets"[17]; 6) „The ability to protect or defend the use of cyberspace from cyber-attacks" (CNSS, 2010); 7) „The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access so as to ensure confidentiality, integrity and availability"[18]; 8) The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets and critical infrastructure"[19]; 9) „The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this"[20]; 10) „The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation"[21]; 11) Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights[22]; 12) The physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on [the country's] physical or economic security or public health or safety[23];

16 E. Amoroso, *Cyber Security*, New Jersey 2006; D.A. Baldwin, *The Concept of Security*, „Review of International Studies" 1997, vol. 23, p. 5–26.

17 *Overview of Cybersecurity. Recommendation ITU-T X.1205*, Geneva 2009.

18 *Emergency Management Vocabulary*, „Terminology Bulletin" 2014, no. 281, http://www.bt-tb.tpsgcpwgsc.gc.ca/publications/documents/urgence-emergency.pdf [access: 15.01.2022].

19 C. Canongia, R. Mandarino, *Cybersecurity: The New Challenge of the Information Society. In Crisis Management: Concepts, Methodologies, Tools and Applications*, Hershey, PA 2014, p. 60–80.

20 *Oxford Online Dictionary*, Oxford 2014, http://www.oxforddictionaries.com/definition/english/Cybersecurity [access: 10.12.2021].

21 *A Glossary of Common Cybersecurity Terminology*, National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security, October 1, 2014, http://niccs.us-cert.gov/glossary#letter_c [access: 16.12.2021].

22 D. Craigen, N. Diakun-Thibault, R. Purse, *Defining Cybersecurity*, „Technology Innovation Management Review" 2014, no. 4, p. 13–21.

23 dhs.gov./topic/critical.infrastuctrure-security [access: 20.12.2021].

13) „Necessarily shifts to contexts and conditions that determine the process by which key actors subjectively arrive at a shared understanding of how to conceptualize and ultimately respond to a security threat"[24].

According to Dan Craigen, Nadia Diakun-Thibault, and Randy Purse the following „dominant terms" need to be examined: i) technological solutions; ii) events; iii) strategies, processes, and methods; iv) human engagement; and v) referent objects (of security).

Ostensibly involve interactions between humans, between systems, and between humans and systems. Protection, in the broadest sense, from all threats, including intentional, accidental, and natural hazards. Any event or activity that misaligns actual (de facto) property rights from perceived (de jure) property rights, whether by intention or accident, whether known or unknown, is a cybersecurity incident.

As the definition of cybersecurity expanded and shifted, more legislative and regulatory subunits claimed some degree of decision-making authority and committees have relied heavily on federal agencies for information about how existing regulations may apply to new attributes of the problem. If regulatory uncertainty is defined as „change in the regulatory process"[25], then changes in how a problem is defined and authority is allocated among regulators fit neatly within that framework.

The second lesson for governance is that diffuse authority leads to piecemeal policy approaches, which in turn require coordination. Issues for which the nature of the problem is uncertain often require flexible responses, coordination, and cooperation; uncertainty about the nature of the problem driven by changes in technology pose additional challenges for governance in managing vulnerability to unanticipated developments and assets and in balancing trial-and-error risk forecasting with accountability[26].

In the context of cybersecurity, law as a form of social engineering is a type of attack wherein the attacker(s) exploit human vulnerabilities by means of social interaction to breach cyber security, with or without the use of technical means and technical vulnerabilities. These human vulnerabilities could stem

24 M.D. Cavelty, *Cyber-Security* [in:] *The Routledge Handbook of New Security Studies*, ed. J.P. Burgess, London 2010, p. 154–162.

25 K. Cook et al., *A Theory of Organizational Response to Regulation: The Case of Hos-pitals*, „Academy of Management Review" 1983, no. 8, p. 193–205.

26 S.A. Adams et al., *How Does Cybersecurity Governance Theory Work When EveryoneIs a Stakeholder?* [in:] *Cybersecurity Governance*, eds. R. Ellis, V. Mohan, Hoboken, NJ 2019, p. 117–136.

from aspects of psychology, cognition, consciousness, thought, behavioural habits, neural reflexes, etc. The social interaction in social engineering is the communication between or joint activity involving two or more human roles. Since cybersecurity involves security issues that exist in electromagnetic equipment, information communication systems, operating data and system applications in cyberspace[27].

To breach cyber security, in general, is to breach the security goals – such as confidentiality, integrity, availability, controllability, auditability, etc.... – of the four basic elements of cyberspace.

These four basic elements are: 1) the Carrier – like the infrastructure, hardware, and software facilities of cyber space; 2) Resources – the objects, data content that flows through the cyber space; 3) Subjects – the main body roles and users, including human users, organizations, equipment, software, websites; 4) Operations – all kinds of activities of processing Resources, including creation, storage, change, use, transmission, display[28].

Obtaining physical access is included in the purpose of social engineering attacks by some studies. Typically, this includes making the victims reveal information, e.g. passwords, giving the adversary illegitimate access to buildings and granting access to restricted areas[29].

Therefore, although cybersecurity tends to be an IT question with amazingly comprehensive technological aspect, there is nonetheless a personal aspect to it. And criminal law in its mens rea requirement needs this personal aspect. Hence, I could conduct that my hypothesis is a valid question.

Cybersecurity may be linked to international criminal law. This is stating the obvious, because cybersecurity needs the world wide web, or some informatical aspect; and in our new world informatics is totally cross-bordered, because in a fragment of second someone could access any world market, any system and cause problems, harms or even criminal acts. In this paper I will try to give a perspective in how cybersecurity mainly understood by me as the

27 B. Fang, *The definitions of fundamental concepts* [in:] *Cyberspace Sovereignty*, New York, NY 2018, p. 1–52.

28 B. Fang, *Define cyberspace security* „Chinese Journal Network Information Security" 2018, vol. 4, no. 1, p. 1–5.

29 H. Hasle et al.: *Measuring resistance to social engineering* [in:] *Information Security Practice and Experience (Lecture Notes in Computer Science)*, Berlin 2005, p. 132–143; Z. Benenson, F. Gassmann, R. Landwirth, *Unpacking spear phishing susceptibility* [in:] *Financial Cryptography and Data Security (Lecture Notes in Computer Science)*, eds. M. Brenner et al., New York, NY 2017, p. 610–627.

combination of the definition given by the Oxford Dictionary and Dan Craigen. Under the criminal actor I will reflect on Kemmerer's definition of intruder.

The Problem

No single treaty exists that is primarily concerned with regulation of the Internet and the key topic of cybersecurity. Although treaties provide (legal) certainty (especially in the eyes of powerful states or states relying on traditional sovereignty concepts), bilateral cybersecurity treaties usually do not live up to the complexity of the issue due to the universality of the Internet, while multilateral treaties can only be attained through lengthy negotiation processes with an uncertain outcome[30].

I will use the basic oxford dictionary definition: „The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this". to highlight the specific problems when it comes to international criminal law. On the following pages I will demonstrate that there is no clear definition on the crimes of crimes, and that it is extremely difficult to put an act or omission under the notion of other inhuman acts. Leaving us with no view on the future, in which throughout the internet the possibility of committing crimes exists.

Where all are guilty, no one is. – Hannah Arendt, *Responsibility and Judgment*
First I need to mention that, although not specifically to cybersecurity, but to international criminal law, it is easy to become a „victim" to a „hero" of some sort[31].

The main problem arises, when it comes to the „crime of crimes"[32], namely genocide in comparison to and with crime against humanity. Curiously enough, the term „crimes against humanity", which provided a catchy title to go along with „crime against peace" and „war crimes", did not make an appearance in the

30 *USA und China wollen Vertrag zur Begrenzung von Cyberangriffen'*, Heise.de, September 20, 2015, https://www.heise.de/security/meldung/USA-und-China-wollen-Vertrag-zur-Begrenzung-von-Cyberangriffen-2822083.html [access: 15.01.2022]; J. Ldsmith, *Cybersecurity Treaties. A Skeptical View*, Hoover Institution Future Challenges Essays, 2011, p. 1–16, http://media.hoover.org/sites/default/files/documents/FutureChallengesGoldsmith.pdf [access: 15.02.2022]; R.S. Litwak, M. King, *Arms Control in Cyberspace?*, Wilson Briefs, Wilson Center Digital Futures Project, 2015, p. 1–7, https://www.wilsoncenter.org/publication/arms-control-cyberspace [access: 15.01.2022].

31 K.M. Clarke, *Affective Justice: The International Criminal Court and the Pan-Africanist Pushback*, Durham 2019.

32 Kambanda, ICTR Trial Chamebr, Judgment, ICTR-97-23, 4 Septemebr 1998, para. 16.

drafting of the Nuremberg Charter until the very last moment. Prior talk had been of „atrocities", „persecutions" and some-times „deportations" (it apparently being understood that these were for the purpose of slave/forced labour)[33].

Genocide and crimes against humanity

Genocide is defined in the Convention on the Prevention and Punishment of the Crime of Genocide 1948 (hereafter referred to as the Genocide Convention) as being the commission of specific acts „with intent to destroy, in whole or in part, a national, ethnical, racial or religious group, as such". I want to demonstrate that when it comes to demonstrating that genocide is not only a special category of crimes against humanity but also that, as a result, it is largely a redundant crime.

The specified acts can be killing members of the group; inflicting bodily or mental harm on members of the group; inflicting conditions of life calculated to bring about the group's destruction; forcible birth control; and the forcible transferal of children[34].

Genocide depends on the existence in the perpetrator's mind of a specific intent to destroy in whole or in part a Convention group by one of the specified methods, alongside the intent to commit the specified act.

Crimes against humanity present a broader range of offences and there is no requirement for a specific group to be targeted; it is sufficient for there to be a widespread or systematic attack committed against a civilian population. The offences that can constitute a crime against humanity include murder, extermination, and enslavement[35]. to which the Statute of the International Criminal Court (ICC) adds apartheid, enforced disappearance, and sexual slavery, etc.

33 R.S. Clark, *Crimes Against Humanity at Nuremberg* [in:] *The Nuremberg Trial and International Law*, eds. G. Ginsburgs, V.N. Kudriavtsev, Dordrecht–Boston 1990, p. 181–194.
34 See the upper defintion olus Convention on the Prevention and Punishment of the Crime of Genocide, 12 January 195 1, Art. 2, 78 U.N.T.S. 277.
35 See the Rome Statue just as much as Art. 5 Statute of the ICTY, Art. 3 Statute of the ICTR.

Persecution as another Inhuman Act and the Mens Rea of Genocide

The essential element of genocide is that the perpetrator intended, by his actions, to destroy in whole or in part a Convention group. Essentially, targeting individuals because of their group membership with a view to destroying that particular group is discriminatory and thus an act of persecution. A hierarchy of the mens rea for international crimes has been described by Clark[36]. In this hierarchy genocide is the crime which requires the highest level of proof of mens rea namely the specific intent, or dolus specialis, to destroy in whole or in part a Convention group. Crimes against humanity require proof that the individual possesses knowledge of the wider context of the crimes for a successful prosecution to result.

As a crime against humanity persecution has three distinct elements. First, there is the occurrence of a discriminatory act; secondly, the occurrence of the act based on the group membership of the victims; and thirdly, „the persecutory act must be intended to cause, and result in, an infringement on an individual's enjoyment of a basic or fundamental [right]"[37].

Count 4(B) of the Nuremberg Indictment specified persecution on 'political, racial, or religious grounds' as a crime against humanity[38]. Persecution is a broad crime which „encompasses a variety of acts, including, inter alia, those of a physical, economic or judicial nature, that violate an individual's right to the equal enjoyment of his basic rights"[39].

In Kupreskic: „[a] lthough individual acts may not be inhumane, their overall consequences must offend humanity in such a way that they may be termed 'inhumane'"[40].

Furthermore, it is not necessary to identify which rights constitute „fundamental rights for the purpose of persecution"[41]. Meaning that the Dolus

36 R.S. Clark, *The Mental Element in International Criminal Law: The Rome Statute of the International Criminal Court and the Elements of Offences'*, „Criminal Law Forum" 2001, no. 3, p. 291–334.

37 Tadić, ICTY Trial Chamber Judgment, IT-94-1, 7 May 1995, para. 715.25.

38 *Count 4 (B), IMT Indictment* [in:] *International Military Tribunal (Nuremberg), Trial of the Major War Criminals Before the International Military Tribunal 14 November 1945–1 October 1946*, vol. 1, Nuremberg 1947, p. 66.

39 Tadić, para. 710.

40 Kupreškić, ICTY Trial Chamber Judgment, 1T-95-16, 14 January 2000, para. 622.

41 Stakić, ibidem, IT-97-24, 31 July 2003, para. 773.

specialis is a civil law term which the ICTR has equated with the common law term of „specific intent"[42].

Article 30 of the ICC Statute establishes the mens rea for the offences over which it has been granted jurisdiction. However, this only renders an individual criminally responsible if the actus reus is committed „with intent and knowledge"[43]. Consequently, it must be proven that the individual accused intended to engage in the criminal act and meant to cause the consequences of his act[44]. In Jelifi. the ICTY Trial Chamber stated that the „'special' intention which [...] characterises his intent to destroy the discriminated group as such, at least in part"[45].

In Akayesu, the Trial Chamber noted the difficulties associated with proving the mens rea of genocide. It found „that intent is a mental factor which is difficult, even impossible, to determine"[46]. Aptel concludes on this subject that „circumstantial" 39 evidence may also be used to establish the requisite intent[47].

In Bagilishema where the Trial Chamber ruled that the „that the use of context to determine the intent of an accused must be counterbalanced with the actual conduct of the [accused]"[48].

Due to its nature persecution is also an umbrella offence under which other crimes against humanity can be committed as noted in Todorovic: „persecution is the only crime enumerated in Art. 5 of the [ICTY] Statute which [...] by its nature [...] may incorporate other crimes"[49].

To the actus reus elements, the two crimes of murder as a form of crime against humanity and genocidal killing are closely linked. In Staki6 extermination was described as „the annihilation of a mass of people"[50].

What distinguishes extermination from genocidal killing is that the former targets not a group but a large number of people. This can be comprised of one

42 Akayesu, ibidem, ICTR-96-4, 2 September 1998, para. 122.
43 Article 30(2)(a-b) Statute of the ICC.
44 Ibidem.
45 Jelisić, ICTY Trial Chamber Judgment, IT-95-10, 14 December 1999, para. 78.
46 Akayesu, para. 523.
47 C. Aptel, *The Intent to Commit Genocide in the Case Law of the International Criminal Tribunal for Rwanda*, „Criminal Law Forum" 2002, no 3, p. 273, 288.
48 Bagilishema, ICTR Trial Chamber Judgment, ICTR-95-I, 7 June 2001, para. 63.
49 Todorović, ibidem, IT-95-9/1, 31 July 2001, para. 32.
50 Stakić, ibidem, IT-97-24, 31 July 2003, para. 641.

act or a number of acts „which contributes to the killing of a large number of individuals"[51], a view supported in Vasiljevic[52].

In Kayishema and Ruzindana the ICTR held that an individual may be prosecuted for the crime of extermination for „a single killing" if that „killing form[s] part of a mass killing event" and that the murder took place in the context of mass killing[53].

In terms of cybersecurity it is interesting to note here that there are proponents of two different types of tests to identifying if indirect intervention has taken place; the overall control test developed by the ICTY in Tadic[54] and confirmed by the ICC in Lubanga[55], on one hand; and the 'effective control' test as developed by the ICJ in the Nicaragua[56] and Bosnia Genocide cases[57]. Regardless, this clearly shows that the Court's hesitance in the use of secondary sources is only to the extent that they do not conflict with its primary ones. Aside from this, it has readily interpreted the Statute though treaty law, general principles and custom as well as referred to the decisions of the ad hoc tribunals.

The notion of other inhuman acts

The Rome Statute of the ICC was devised with the awareness that „the most serious crimes of concern to the international community as a whole must not go unpunished and that their effective prosecution must be ensured…"[58].

51 G. Mettraux, *International Crimes and the Ad Hoc Tribunals*, Oxford, 2006, p. 176.
52 Vasiljević, ICTY Trial Chamber Judgment, IT-98-32, 25 February 2004, para. 229.
53 Kayishema and Ruzindana, ibidem, ICTR-95-1, 1 June 2001, para. 147.
54 ICTY, Prosecutor v. Tadić, Case No. IT-94-A, Judgment, 15 July 1999, para. 145.
55 Situation in the Democratic Republic of the Congo (Prosecutor v Thomas Lubanga Dyilo) (Decision on the Confirmation of Charges) (ICC-01/04-01/06). 28 January 2007, par. 210, 211; Situation in the Democratic Republic of the Congo (Prosecutor v. Thomas Lubanga Dyilo) (Judgement Pursuant to Art. 74 of the Statute) (14 March 2012) (ICC-01/04-01/06-2842, para. 541).
56 ICJ, Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Judgment, 27 June 1986 (Merits), para. 115.
57 ICJ, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, 27 February 2007, para. 406 and 413.
58 Rome Statute Preamble as opinion juris.

Another of its goals is not to just prosecute individuals for the crimes they have committed, but also to deter such acts from occurring in the future[59].

Whether or not the ICC functions as a deterrent to the commission of war crimes, genocide or crimes against humanity is an area which is often of debate. However, before one can even ask such a question it is important to understand what „crimes of concern to the international community" entails. It is true that the Rome Statute provides an extensive list of crimes under which it has jurisdiction, but it cannot be assumed that all crimes which are of concern to the international community will always fall within the scope of those already enumerated within the Statute.

The eleventh (and last) category of offences listed in the first paragraph of this provision refers to „[o] ther inhumane acts of a similar character intentionally causing great suffering, or serious injury to body or to mental or physical health".

The first to mention is the forced marriage. Forced marriage in the world of dark web, and compromising photos is easily accessible to the perpetrator. I will only discuss forced marriage in relation to international criminal law such as that which occurred in Uganda, Mozambique, Sierra Leone, Democratic Republic of the Congo and Rwanda. The writer is aware that 'forced marriage' is a term which has been used in reference to other situations such as bride wealth and bride inheritance but to avoid confusion it will not be labelled as such. These are instead understood in this chapter to fall within the scope of arranged marriages that do not adhere to international human rights standards but do not meet the requirements of international criminal law. That is, they do not occur as a part of a widespread or systematic attack against a civilian population[60].

To begin it is necessary to understand the importance in identifying marriage as a general principle of law. International criminal tribunals largely tend to opt in favour of using customary international law when progressively interpreting the scope of a given crime within their statute[61]. The right to marriage itself is recognized within a plethora of domestic legal systems. It is deemed as a fundamental right in the EU Charter of Fundamental Rights

59 Ibidem.

60 K. Chantler, G. Gangoli, M. Hester, *Forced marriage in the UK: Religious, cultural, economic or state violence?*, „Critical Social Policy" 2009, vol. 29, no. 4.

61 Prosecutor V. Zoran Kupreškić et al. (Trial Judgment), ICTY Trial Chamber Judgment, IT-95-16-T, 14 January 2000, para. 591.

Art. 9 which states „The right to marry and the right to found a family shall be guaranteed in accordance with the national laws governing the exercise of these rights". Italy, France and Germany just – as much as Hungary and Poland – have all adopted or include similar rights to marriage within their constitution or respective civil codes[62].

In the USA The right has also been affirmed in Planned Parenthood of Southeastern Pennsylvania v. Casey which declared, „these matters, involving the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy, are central to the liberty protected by the Fourteenth Amendment. At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life"[63].

Marriage is not only recognized as an important societal institution within domestic legal systems, but also as a fundamental right of the individual at the international level. Historically, rights of the family during wartime have been widely recognized, such as in the Lieber Code of 1863[64], the Brussels Declaration of 1874[65], the 1907 Hague Convention[66], and Geneva Conventions (IV) relative to the Protection of Civilians Persons in Times of War[67].

While marriage itself can be considered as a general principle of international law its implications on the status of forced marriage may still be of question. Justice Julia Sebutinde and Justice Teresa Doherty of the SCSL in their respective concurring and dissenting opinions to the Armed Forces Revolutionary Council (AFRC) Trial Chamber Judgment as well as the ARFC Appeals Chamber in their judgment recognized that the legal status of

62 Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, Art. 9; Constitution of Italy, 22 December 1947, Art. 29; Basic Law for the Federal Republic of Germany, 23 May 1949, Art. 6(1); Code Civil, 7 January 1999, Art. 146.

63 Planned Parenthood of Southeastern Pennsylvania v. Casey. 505 U.S. 833 (1992).

64 Instructions for the Government of Armies of the United States in the Field (Lieber Code), 24 April 1863, Art. 24.

65 Project of an International Declaration concerning the Laws and Customs of War (Brussels Declaration), 27 August 1874, Art. 38.

66 Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land (Hague Convention), 18 October 1907, Art. 46.

67 Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), 12 August 1949, 75 UNTS 287, Art. 27.

marriage was not meant to impart any implications upon the criminalization of arranged marriages[68].

Sexual slavery, similar to that of forced marriage, is a relatively new crime in terms of its recognition as a distinct form of slavery in the statutes of international criminal tribunals. It was first adopted as a crime against humanity under the Rome Statute Art. 7(1)(g). It serves as a general definition of the act of slavery based off the 1926 Slavery Convention and Supplementary Convention on the Abolition of Slavery, the Slave Trade, and Institutions and Practices Similar to Slavery of 1956[69]. Unfortunately, sexual slavery is a possible act to commit, with the hacking of guarding systems, and through the installation of different cameras.

Other inhuman act would be also ethnic cleansing, „Ethnic cleansing" quite often is accomplished through enacting discriminatory and repressive legislation, harassment, death threats, forced removal from one's work, refusal of medical treatment, non-consensual publication of a group or individuals private information including religious affiliation and ethnicity, as well as other acts[70]. Yet ethnic cleansing is without merit to cybersecure aspects, since the mens rea is literally impossible to prove.

Bibliography

A Glossary of Common Cybersecurity Terminology, National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security, October 1, 2014, http://niccs.us-cert.gov/glossary#letter_c [access: 16.12.2021].

Adams S.A. et al., *How Does Cybersecurity Governance Theory Work When EveryoneIs a Stakeholder?* [in:] *Cybersecurity Governance*, eds. R. Ellis, V. Mohan, Hoboken, NJ 2019.

Amoroso E., *Cyber Security*, New Jersey 2006.

Aptel C., *The Intent to Commit Genocide in the Case Law of the International Criminal Tribunal for Rwanda*, „Criminal Law Forum" 2002, no. 3.

68 Prosecutor V. Alex Tamba Brima, Brima Bazzy Kamara, and Santigie Borbor Kanu. (Separate Concurring Opinion of the Honorable Justice Julia Sebutinde Appended to the judgement pursuant to Rule 88 (c)), Special Court for Sierra Leone (SCSL), SCSL-04-16-T, 20 June 2007, para. 8–12; Prosecutor v. Alex Tamba Brima, Brima Bazzy Kamara, and Santigie Borbor Kanu (Appeals Judgment), Special Court for Sierra Leone (SCSL), SCSL-2004-16-A, 22 February 2008, para. 194; Prosecutor v. Alex Tamba Brima, Brima Bazzy Kamara, and Santigie Borbor Kanu [Partly Dissenting Opinion of Justice Doherty on Count 7 (Sexual Slavery) and Count 8('Forced Marriages')], Special Court for Sierra Leone (SCSL), SCSL-04-16-T, 20 June 2007, para. 36.

69 K. Dormann, *Elements of war crimes under the Rome statute of the International criminal court: sources and commentary*, Cambridge 2003, p. 327–328.

70 D. Petrovic, *Ethnic Cleansing – an Attempt at Methodology* „European Journal of International Law" 1994, vol. 5, p. 345–346.

Baldwin D.A., *The Concept of Security*, „Review of International Studies" 1997, vol. 23.
Benenson Z., Gassmann F., Landwirth R., *Unpacking spear phishing susceptibility* [in:] *Financial Cryptography and Data Security (Lecture Notes in Computer Science)*, eds. M. Brenner et al., New York, NY 2017.
Canongia C., Mandarino R., *Cybersecurity: The New Challenge of the Information Society. In Crisis Management: Concepts, Methodologies, Tools and Applications*, Hershey, PA 2014.
Cavelty M.D., *Cyber-Security* [in:] *The Routledge Handbook of New Security Studies*, ed. J.P. Burgess, London 2010.
Chang F.R., *Guest Editor's Column*, „The Next Wave" 2012, vol. 19, no. 4.
Chantler K., Gangoli G., Hester M., *Forced marriage in the UK: Religious, cultural, economic or state violence?*, „Critical Social Policy" 2009, vol. 29, no. 4.
Clark R.S., *Crimes Against Humanity at Nuremberg* [in:] *The Nuremberg Trial and International Law*, eds. G. Ginsburgs, V.N. Kudriavtsev, Dordrecht–Boston 1990.
Clark R.S., *The Mental Element in International Criminal Law: The Rome Statute of the International Criminal Court and the Elements of Offences'*, „Criminal Law Forum" 2001, no. 3.
Clarke K.M., *Affective Justice: The International Criminal Court and the Pan-Africanist Pushback*, Durham 2019.
Cook K. et al., *A Theory of Organizational Response to Regulation: The Case of Hos-pitals*, „Academy of Management Review" 1983, no. 8.
Craenig D., Diakun-Thibault N., Purse R., *Defining Cybersecurity*, „Technology Innovation Management Review" 2014, no. 4.
dhs.gov./topic/critical.infrastuctrure-security [access: 20.12.2021].
Dormann K., *Elements of war crimes under the Rome statute of the International criminal court: sources and commentary*, Cambridge 2003.
Emergency Management Vocabulary, „Terminology Bulletin" 2014, no. 281, http://www.bt-tb.tpsgcpwgsc.gc.ca/publications/documents/urgence-emergency.pdf [access:15.01.2022].
Fang B., *Define cyberspace security*, „Chinese Journal Network Information Security" 2018, vol. 4, no. 1.
Fang B., *The definitions of fundamental concepts* [in:] *Cyberspace Sovereignty*, New York, NY 2018.
Hasle H. et al., *Measuring resistance to social engineering* [in:] *Information Security Practice and Experience (Lecture Notes in Computer Science)*, Berlin 2005.
Heller K., *The Rome Statute of the International Criminal Court* [in:] *The Handbook of Comparative Criminal Law*, eds. K. Heller, M. Dubber, Redwood City 2010.
Kemmerer R.A., *Cybersecurity* [in:] *Proceedings of the 25th IEEE International Conference on Software Engineering, 2003*, http://dx.doi.org/10.1109/ICSE.2003.1201257 [access: 25.01.2022].
Ldsmith J., *Cybersecurity Treaties. A Skeptical View*, Hoover Institution Future Challenges Essays, 2011, http://media.hoover.org/sites/default/files/documents/FutureChallengesGoldsmith.pdf [access: 15.02.2022].
Lewis J.A., *Cybersecurity and Critical Infrastructure Protection*, Washington, DC 2006.
Litwak R.S., King M., *Arms Control in Cyberspace?*, Wilson Briefs, Wilson Center Digital Futures Project, 2015, https://www.wilsoncenter.org/publication/arms-control-cyberspace [access: 15.01.2022].
Mettraux G., *International Crimes and the Ad Hoc Tribunals*, Oxford 2006.
Overview of Cybersecurity. Recommendation ITU-T X.1205, Geneva 2009.
Oxford Online Dictionary, Oxford 2014, http://www.oxforddictionaries.com/definition/english/Cybersecurity [access: 10.12.2021].
Petrovic D., *Ethnic Cleansing – an Attempt at Methodology*, „European Journal of International Law" 1994, vol. 5.
Schmitt M.N., Vihul L., *The Nature of International Law Cyber Norms*, „Tallinn Paper" 2014, no. 5.

USA und China wollen Vertrag zur Begrenzung von Cyberangriffen', Heise.de, September 20, 2015, https://www.heise.de/security/meldung/USA-und-China-wollen-Vertrag-zur-Begrenzung-von-Cyber-angriffen-2822083.html [access: 15.01.2022].
Workman S., *The Dynamics of Bureaucracy in the U.S. Government: How Congress and Federal Agencies Process Information and Solve Problems*, New York 2015.
Workman S., Shafran J., Bark T., *Problem Definition and Information Provision by Federal Bureaucrats*, „Cognitive Systems Research" 2017, vol. 43.
Ziolkowski K., *General Principles of International Law as Applicable in Cyberspace* [in:] *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, ed. K. Ziolkowski, Tallinn 2013.

Cyberbezpieczeństwo a międzynarodowe prawo karne

Streszczenie

Autor artykułu szczegółowo omawia możliwość popełniania przestępstw, które podlegałyby Statutowi rzymskiemu, w kontekście pojęcia cyberbezpieczeństwa. Autor dochodzi do wniosku, że niezbędne są szeroko zakrojone badania empiryczne i rozwiązania wielu kwestii wskazanych w artykule. Po pierwsze, należy wypracować możliwą do przyjęcia definicję cyberbezpieczeństwa, żeby kontynuować ten proces oraz zrozumieć świat i możliwości, jakie dla nas stwarza. Ponadto Statut rzymski z 1998 roku wymaga aktualizacji, ponieważ Internet stwarza niespotykane dotąd możliwości, a międzynarodowe orzecznictwo nie jest w stanie poradzić sobie z tak odmiennymi działaniami. Autor wskazuje na konieczność podjęcia kolejnych „procesów norymberskich", nowej formy rozwiązań dla świata i przestępczości, z jaką wcześniej nie mieliśmy do czynienia. Potrzebujemy rewolucji teoretycznej i prawnej podobnej do tej, jaka nastąpiła po II wojnie światowej i po trybunałach karnych *ad hoc* takich, jak Międzynarodowy Trybunał Karny dla byłej Jugosławii (ICTY), Międzynarodowy Trybunał Karny dla Ruandy (ICTR) czy Międzynarodowy Trybunał Karny dla Sierra Leone. Autor ma nadzieję, że ten krótki artykuł podsumowujący będzie punktem wyjścia do przyszłych referatów i konferencji, które przyniosą kolejne rozwiązania i sposoby reagowania na dwie kwestie, tj. konieczność wypracowania ostatecznej definicji cyberbezpieczeństwa oraz wskazanie jej interpretacji w kontekście klasycznego pojęcia międzynarodowego prawa karnego. Jeżeli rozstrzygnięcie tych kwestii okaże się niemożliwe, to autor proponuje powołanie panelu na szczeblu międzynarodowym lub w Grupie Wyszehradzkiej, który skupi się na reorganizacji zwyczajowego międzynarodowego prawa karnego na gruncie Statutu rzymskiego lub na nieustannie ewoluującej definicji cyberbezpieczeństwa.

Słowa kluczowe: cyberbezpieczeństwo, prawo karne, prawo międzynarodowe, międzynarodowe prawo karne, ludobójstwo, inne nieludzkie czyny