UDK 341.3:343.222]:004
Original scientific paper

INDIVIDUAL CRIMINAL RESPONSIBILITY OF NON-STATE ACTORS OPERATING IN CYBERSPACE FOR WAR CRIMES UNDER THE ICC STATUTE*

Giulia Gabrielli, PhD, Post-doctoral Research Fellow
University of Milan, Department of International,
Legal, Historical and Political Studies
Via Conservatorio 7, 20 122 Milan, Italy
giulia.gabrielli@unimi.it

ABSTRACT

Contemporary armed conflict has witnessed an increased employment of digital technologies in the conduct of hostilities. While there is broad consensus on the full applicability of the rules and principles of international humanitarian law (IHL) to the "fifth domain" of warfare, many issues remain debated. More specifically, digital technologies allow a wide range of actors other than States – such as individuals, "hacktivists", criminal groups, non-State armed groups – to play a role in the hostilities and engage in cyber operations that have the potential of harming civilians or damaging civilian infrastructure and that may amount to serious violations of IHL.

Against this backdrop, this paper seeks to examine the legal grounds upon which hostile cyber operations carried out by non-State actors (NSAs) could constitute war crimes, thus entailing their individual criminal responsibility under international law. Hence, the analysis will focus on the applicability of the war crimes provisions of the Rome Statute of the International Criminal Court (ICC) to such operations, with a view to identifying the prerequisites necessary to trigger the ICC's jurisdiction.

To this end, the first part will focus on the increased involvement of NSAs in the conduct of hostilities by cyber means, taking the recent conflict between Russia and Ukraine as a pertinent case study. Subsequently, the paper will explore the conditions necessary for the application of Article 8 of the ICC Statute, with special attention devoted to those aspects that are deemed particularly problematic in light of the participation of NSAs in armed conflict. Finally, the paper seeks to highlight the limits of possible future investigations of cyber conducts possibly amounting to war crimes. These encompass not only issues of admissibility, but also the statu-

* This paper is co-funded by the Erasmus+ Programme of the European Union. The paper reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

tory limits of the Rome Statute when it comes to war crimes provisions applicable to non-international armed conflicts.

***Keywords**: cyberwarfare, International Criminal Court (ICC), individual criminal responsibility, international humanitarian law, non-State actors, war crimes*

1. INTRODUCTION

In the last decades, the role of information and information technology (IT) has significantly expanded to pervade all aspects of human interaction. A variety of entities, including States and individuals, consistently rely on communication technologies to perform several functions, which range from business operations to food, water, or energy distribution, as well as transportation, finance, health care and manufacturing.

Against this backdrop, armed conflict is not exempt from the ubiquity of new technologies. Computers, computer systems and networks are increasingly used by military forces, both in their ordinary organizational activities and logistics, but also, and more notably, in the conduct of hostilities.[1] The use of means and methods of warfare that take advantage of digital technologies such as autonomous weapons systems, artificial intelligence, precision-guided munitions, etc. allow belligerents to direct their attacks with more precision, to better coordinate the action of military forces on the field, and to make informed decisions in targeting. These hence might have a positive impact on the protection of civilians during armed conflict since they might allow belligerent parties to minimize collateral damage and to reduce the need to resort to armed force to achieve certain military goals.[2]

The impact of new technologies on warfare is not strictly limited to the conduct of hostilities *per se* but extends to the investigation of human rights violations as well, by contributing to the creation of open-source repositories of digital evidence that are captured, for instance, by the mobile phones of eyewitnesses, victims and perpetrators and posted on social media. The use of digitally derived evidence[3] in criminal proceedings necessarily involves potential risks but might also be usefully

---

1 Lin, H., *Cyber conflict and international humanitarian law*, International Review of the Red Cross, Vol. 94, No. 886, 2012, p. 516.

2 *Ibidem*; International Committee of the Red Cross, *International Humanitarian Law and the challenges of contemporary armed conflicts - Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions*, 22 November 2019, Report, p. 26.

3 For a debate on the challenges and opportunities of the use of digital and open-source evidence, see *To What Extent Can Cyber Evidence Repositories, and Digital and Open-Source Evidence, Facilitate the Work of the OTP, and the ICC More Generally?*, ICC Forum, 2020, [https://iccforum.com/cyber-evidence], Accessed 15 November 2022.

integrated into international criminal investigations and prosecutions and represent new opportunities for justice.[4]

Without prejudice to the unprecedent advantages offered by IT in the framework of armed conflict and in the legal and accountability processes, new cyber technologies also present many risks and potential threats, in particular when used maliciously. Their affordability and relative accessibility allow a wide range of actors other than States, such as individual hackers, criminal groups, non-State armed groups and other non-State actors, to play a role in the hostilities and to cause considerable damage to the other actors involved, including militarily superior and better equipped States.[5] In this context, the increased involvement of non-State actors in armed conflict necessarily poses the issue of their increased capacity to engage in cyber operations that might result in harming civilians or causing damage to civilian infrastructure with potentially disastrous consequences. Although it does not seem that their involvement in the hostilities has given origin to serious humanitarian consequences to date, the development of increasingly sophisticated capabilities in cyberwarfare could potentially cause serious consequences for civilians and civilian infrastructure that might amount to serious violations of International Humanitarian Law (IHL), hence giving rise to the individual criminal responsibility of the perpetrator(s).

The International Committee of the Red Cross (ICRC) has consistently emphasized its humanitarian concern in respect to cyberwarfare,[6] which – due to its nature – has the potential of severely affecting civilians and civilian infrastructure for several reasons. Firstly, due to the increased reliance of civilian infrastructure on computer systems, cyber attacks may have a significant impact on the health-care sector and hospital systems, as well as critical installations, including the electrical networks, dams, nuclear plants, banking systems, railroads and air traffic. Secondly, due to the growing digitization, military and civilian networks are increasingly

---

4 Since 2015, the Office of the Prosecutor (OTP) of the International Criminal Court has relied on digital open-source content in the investigation of a number of cases, including satellite imaging collected by Google Earth in *Banda Jerbo*, *Abu Garda* and *Al Mahdi*, video materials and posts on social media in *Al-Werfalli* and evidence of wire transfer and pictures from Facebook in *Bemba et al.* See, in general, Costello, R. Á., *Facilitating the Use of Open Source Evidence at the International Criminal Court: Authentication and the Problem of Deepfakes*, ICC Forum, 2020 [https://iccforum.com/cyber-evidence#-Costello], Accessed 15 November 2022.

5 Roscini, M., *Cyber Operations and the Use of Force in International Law*, Oxford, 2014, pp. 1-2. See also Missiroli, A., *Present Tense: Cyber Defence Matters*, in: Pawlak, P; Delerue, F. (eds.), A Language of Power? Cyber Defence in the European Union, Chaillot Paper/176, November 2022, p. 14, arguing that "digital technologies have dramatically lowered the entry barriers for new threat actors" through the so-called 'democratisation' effect.

6 Gisel L.; Olejnik, L. (eds.), *The potential human cost of cyber operations*, International Committee of the Red Cross, 2018, Report.

interconnected. On the one side, most civilian cyber infrastructure, or civilian infrastructure that relies on cyberspace, e.g. undersea fibre-optic cables, satellites, routers or nodes, may also be used by military networks and serve military purposes. Conversely, civilian air traffic control, vehicles and shipping are provided with navigation systems relying on global navigation satellite system (GNSS) satellites (e.g. BeiDou, GLONASS, GPS and Galileo), which may simultaneously be used by the military.

The implications of this growing interconnectivity are twofold. First, although there exist networks that are specifically designed for the exclusive use of the military, it is almost impossible in most cases to distinguish between cyber infrastructures that serve purely civilian and purely military purposes. Second, the interconnectivity and the 'dual use' of cyber infrastructures implies that cyber attacks directed against military targets may have effects that cannot be confined. This is the case of malwares, including viruses or worms, which – if uncontrollable – may spread indiscriminately among several systems and networks, regardless of their civilian or military nature, with possible repercussions on essential civilian infrastructure.[7]

Against the risks posed by cyber operations during armed conflict, this paper seeks to examine the legal grounds under which a hostile operation led by non-State actors could entail their international criminal responsibility under International Criminal Law (ICL). Namely, the analysis will focus on the possible application of the Rome Statute of the International Criminal Law (ICC) to such operations, with a view to examining the conditions necessary to trigger the Court's jurisdiction with respect to the provisions relating to war crimes. The paper is structured as follows: the first part will deal with the increased involvement of non-State actors in armed conflict by cyber means, by examining by way of example the recent conflict between Russia and Ukraine. Secondly, after some preliminary remarks on the scope of the present research, the attention will be drawn on the conditions of application of the Rome Statute, especially those which are deemed particularly problematic in light of the participation of NSA in armed conflict by cyber means and the issues that may arise.

---

7 See, Gisel, L.; Rodenhäuser, T.; Dörmann, K., *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, International Review of the Red Cross, Vol. 102, No. 913, 2020, p. 320; Droege, C., *Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians,* International Review of the Red Cross, Vol. 94, No. 886, 2012, pp. 538-539.

2. THE INVOLVEMENT OF NON-STATE ACTORS IN THE CONDUCT OF HOSTILITIES BY CYBER MEANS

On 26 February 2022, in response to Russian invasion of Ukrainian territory that had begun on the 24th, Ukraine's Minister of Digital Transformation, Mykhailo Fedorov, announced with a tweet the creation of an "IT army", and called for the participation of cyber specialists from all over the world to join the "fight on the cyber front" against Russia. Thousands of people reportedly responded to the call from the Ukrainian government, which asked for the assistance of IT professionals and hackers to help defending Ukraine's infrastructure from Russian cyber-attacks, and to conduct hostile offensive cyber operations against Russia.[8] With the aim of coordinating the "IT Army", the Ukrainian government created a Telegram channel to instruct its almost 200,000 followers to use cyber and DDoS (Distributed Denial of Service)[9] attacks against a list of websites of Russian or Russian-affiliated targets, including for instance Russian banks and corporations such as Gazprom, but also government agencies, storage devices, and support for critical infrastructure.[10]

Aside from the "IT Army", other Ukrainian hacking collectives, which included for instance hackers from Ukrainian cybersecurity companies and firms, organized in self-managed cyber teams, coordinating their efforts autonomously on private-messaging channels.[11] Their cyber activities, endorsed – and to an extent even coordinated – by the government, reportedly aimed at carrying out a number

---

8 Holland, S.; Pearson, J., *US, UK: Russia responsible for cyberattack against Ukrainian banks*, Reuters, 2022 [https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/], Accessed November 2022; Schectman, J.; Bing, C., *Ukraine calls on hacker underground to defend against Russia*, Reuters, 2022, [https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/], Accessed November 2022.

9 Distributed Denial of Service (DDoS) is a technique that employs multiple computing devices (e.g., computers or smartphones), such as the bots of a 'botnet' (a network of compromised computers remotely controlled by an intruder used to conduct coordinated cyber operations), to render a certain computer system or computer systems unavailable to their users. *See* Schmitt, M. N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017, Glossary definitions, p. 563 *et seq*. The Tallinn Manual 2.0 is a non-legally binding scholarly work crafted by an International Group of Experts and is considered one of the most authoritative resources regarding the applicability of international law in the cyber context. This contribution draws extensively from the legal position of the Experts in the Tallinn Manual, although occasionally diverging from their views.

10 Goodin, D., After *Ukraine recruits an "IT Army," dozens of Russian sites go dark*, Arstechnica, 2022, [https://arstechnica.com/information-technology/2022/02/after-ukraine-recruits-an-it-army-dozens-of-russian-sites-go-dark/] Accessed November 2022.

11 Cerulus, L., *Kyiv's hackers seize their wartime moment*, Politico, 2022 [https://www.politico.eu/article/kyiv-cyber-firm-state-backed-hacking-group/], Accessed November 2022.

of offensive cyber operations, ranging from attacks against Russian websites and mobile applications to make them unavailable, to the disruption of Russian war propaganda. Moreover, these hackers reportedly engaged in identifying vulnerabilities in the Russian service systems, e.g., telecommunication, banking, energy firms, transportation and logistics services, with the purpose of transmitting the information to the Ukraine's cyber forces for the execution of their attacks.[12]

The efforts in responding to Russian invasion through cyber means was also undertaken by a number of cyber collectives composed of like-minded individuals who spontaneously decided to engage in the conflict through cyber means. These activist groups of hackers, known as "hacktivists", were increasingly involved in the Ukrainian-Russian conflict,[13] at least in its earliest phases. Among them, the notorious collective Anonymous publicly declared "cyber war against the Russian government"[14] and contextually started claiming responsibility for a series of hostile cyber incidents, including DDoS attacks, targeting governmental websites and databases, with subsequent shutdowns and malfunctions as well as leak of sensitive data and documents. Soon afterwards, other groups of hacktivists such as "Squad303"[15] and "NB65",[16] reportedly affiliated with Anonymous, claimed responsibility for the breach of several databases and data leakage.

Aside from IT specialists' and hackers' engagement in armed conflict, new technologies also allowed civilians who do not have particular expertise to become involved in the hostilities, for instance by downloading mobile apps that allow them to report the location of incoming missiles and other enemy air threats to Ukrainian forces.[17]

---

12 *Ibid.*

13 Koloßa, S., *The Dangers of Hacktivism How Cyber Operations by Private Individuals May Amount to Warfare*, 2022, [https://voelkerrechtsblog.org/the-dangers-of-hacktivism/], Accessed 4 February 2023.

14 Milmo, D., *Anonymous: the hacker collective that has declared cyberwar on Russia*, The Guardian, 2022 [https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia], Accessed November 2022.

15 *Who is Squad303 that is attacking Russia with Text Messages*, The Tech Outlook, 2022, [https://www.thetechoutlook.com/news/new-release/software-apps/who-is-squad303-that-is-attacking-russia-with-text-messages/] Accessed November 2022.

16 Johnson, B., *Hackers Turn Conti Ransomware Against Russia as Twitter Suspends Some Anonymous Accounts*, HomelandSecurity Today, 2022, [https://www.hstoday.us/subject-matter-areas/cybersecurity/hackers-turn-conti-ransomware-against-russia-as-twitter-suspends-some-anonymous-accounts/] Accessed November 2022.

17 The data collected and reported through the app, called "ePPO", reportedly allowed Ukrainian forces to shoot down a Russian cruise missile targeting critical infrastructure. It must be here noticed that mobile applications as a defensive tool have also been used in other situations. This is the case of "Sentry", used to warn civilians of imminent indiscriminate Syrian and Russian air strikes in Syria. *See* Schmitt, M. N.; Biggerstaff, W. C., *Ukraine Symposium – Are Civilians Reporting With Cell Phones Directly Par-*

In the broader picture, the involvement of entities other than States in the conduct of contemporary hostilities by cyber means is not a new phenomenon. New information technologies indeed have led to a democratization effect[18] that has allowed a variety of non-State actors (NSA), including armed groups, informal collectives of "hacktivists", and lone individuals, to conduct offensive cyber operations, including *inter alia* cyber-attacks and cyber exploitation,[19] with relative ease. Their structure, size, and internal organization vary significantly and so does their motivation: they may act for pure financial gain, as well as for personal, religious or political reasons.[20] As things stand as present, it appears that – among NSAs – cyber operations are most frequently conducted by criminal organizations mainly for economic purposes. Conversely, terrorist groups and militias seem to have limited their use of cyberspace to primarily operational purposes, recruitment, and funding.[21] The legal classification of online collectives and group of hackers has been the object of thorough discussions, in particular with regards to their qualification under IHL and the legal consequences that such qualification might entail.[22]

---

ticipating In Hostilities?, 2022, [https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities/] Accessed 20 February 2023; Schmitt, M. N., *Ukraine Symposium – Using Cellphones To Gather and Transmit Military Information, A Postscript*, 2022, [https://lieber.westpoint.edu/civilians-using-cellphones-gather-transmit-military-information-postscript/] Accessed 20 February 2023.

18 Missiroli, *op. cit.*, note 5.

19 "Cyber exploitation" refers to a variety of actions that are aimed at penetrating computer systems or networks used by an adversary with the purpose of obtaining information that would otherwise not be disclosed. Lin, *op. cit.*, note 1, p. 519.

20 Non-state actors may be informally classified according to their size, structure and motivation. Individual hackers might be formally or informally employed in States' armed forces units, or hired by States to conduct specific operations, or act alone. Criminal organizations may be driven to launch cyber-operations by financial interests and be involved in illegal activities related to cybercrimes. Cyber "mercenaries", whose definition does not correspond to the notion of mercenaries under IHL, are highly skilled hackers who might be hired by the public or private sector to conduct specific cyber-attacks, and are driven solely by financial motivations. Hacktivists are individuals and online collectives who are driven by political or ideological motives and are normally characterized by a loose structure. See, more specifically, Bussolati, N., *The Rise of Non-State Actors in Cyberwarfare*, in Ohlin, J., D.; Govern, K.; Finklestein, C. (eds.), *Cyberwar: Law and Ethics for Virtual Conflicts*, Oxford University Press, Oxford, 2015, pp. 106-111.

21 Missiroli, *op. cit.*, note 5, pp. 17-18.

22 See, for instance, Buchan, R., *Cyber Warfare and the Status of Anonymous under International Humanitarian Law*, Chinese Journal of International Law, 2016, Vol. 15, No. 4, pp. 741-772; Stiano, A., *L'intervento di Anonymous nel conflitto tra Russia e Ucraina: Alcune riflessioni sullo status giuridico degli* hacker *attraverso il prisma del diritto internazionale umanitario*, Ordine internazionale e diritti umani, No. 4, 2022, pp. 982-1000.

For the purposes of our analysis, however, the attention will be limited to those cyber operations conducted by NSAs in the framework of armed conflict, which may entail the individual criminal responsibility under international law, thus excluding the cyber activities that do take place outside of such context, for instance those taking place in peacetime, and those occurring during hostilities, but which do not have a nexus with them (e.g. if motivated solely by profit).[23] Whereas cyber operations are broadly defined as "[t]he employment of cyber capabilities to achieve objectives in or through cyberspace"[24], when they are employed by military entities or to achieve military goals, they may amount to military cyber operations, or "cyber warfare".[25] As will be more accurately discussed below, although cyber operations may be conducted during peacetime or during hostilities, IHL is only applicable to cyber operations that are related to an international or non-international armed conflict.[26]

3. APPLICABILITY OF ICC'S WAR CRIMES PROVISIONS TO CYBER OPERATIONS: CONDITIONS AND LIMITS

Under Article 8 of the Rome Statute, the ICC has jurisdiction with respect to war crimes, when committed in the context of both international armed conflicts (IACs) and non-international armed conflicts (NIACs).[27] In order for a cyber conduct to amount to a war crime falling within the jurisdiction of the ICC, a few conditions are required. In the first place, such conduct must be committed during an armed conflict, whether international or non-international in character, and shall have a nexus to it. Secondly, the cyber conduct must be committed either in the territory of or by a national of a State that is party to the ICC or that has

---

23 According to Lin, the majority of offensive cyber operations up to now have been allegedly conducted by sub-national parties for financial reasons, especially those concerning cyber exploitation. When discussing the activities unrelated to an ongoing armed conflict that would not be governed by IHL, the Experts in the Tallinn Manual offer the example of a private corporation engaged in the theft of intellectual property over a competitor in the enemy State in order to achieve a market advantage. Lin, *op. cit.*, note 1, pp. 519-520; Schmitt, *op.cit.*, note 9, p. 377.

24 Schmitt, *op.cit.*, note 9, Glossary definition, p. 564.

25 Ducheine, P. A. L.; Pijpers, B. M. J., *The notion of cyber operations*, in Tsagourias N.; Buchan, R., (eds.) Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, Cheltenham, 2021, pp. 290-291; Ambos, K., *Cyber-Attacks as International Crimes under the Rome Statute of the International Criminal Court?*, ICC Forum, 2022, [https://iccforum.com/cyberwar#Ambos] Accessed 20 February 2023.

26 Rule 80 of the Tallinn Manual 2.0 states that "[c]yber operations executed in the context of an armed conflict are subject to the law of armed conflict." Schmitt, *op. cit.*, note 9, p. 375.

27 UN General Assembly, Rome Statute of the International Criminal Court (last amended 2010), 17 July 1998 (Rome Statute), Article 8(1).

accepted its jurisdiction. Thirdly, it must involve the material and mental elements of the crimes under the Rome Statute and must be sufficiently grave in nature.[28]

The paragraphs below will attempt to consider some of these conditions in light of the peculiar issues and problems posed by the case under examination, that is the participation of NSA in hostilities by cyber means, and to discuss their possible persecution for war crimes under the Rome Statute.

3.1. The cyber operation must be carried out "in the context of and in association with the armed conflict"

The first pre-requisite for IHL to apply, and for a war crime to be committed, is the existence of a situation of armed conflict. Indeed, for a possible prosecution of a cyber operation as a war crime in accordance with Article 8 of the Rome Statute, it must be established beyond reasonable doubt that said cyber operation was conducted in the context of or in association with an international (IAC) or non-international armed conflict (NIAC).[29]

Neither IHL nor the Rome Statute provide for a definition of 'armed conflict'. Traditionally, reference is made to the jurisprudence of the International Criminal Tribunal for the Former Yugoslavia (ICTY), whose Appeals Chamber (AC) held in *Tadić* that an IAC exists "whenever there is a resort to armed force between States", whereas a NIAC occurs in case of "protracted armed violence between governmental authorities and organized armed groups or between such groups within a State".[30] IHL hence applies from the initiation of the hostilities and ceases to apply at the cessation of active hostilities or at the general close of military

---

[28] It must be noted that Article 8 of the Rome Statute states that the Court shall have jurisdiction over war crimes, "in particular when committed as part of a plan or policy or as part of a large-scale commission of such crimes". The plan, policy, or the large-scale commission of crimes is not a stringent prerequisite, but it falls within the discretionary power of the Court to also consider crimes that are not committed as part of a plan, policy, or large-scale commission. Rome Statute, Article 8 para. 1; Cottier, M., *Article 8, Part I: Introduction/General Remarks*, in Triffterer, O.; Ambos, K. (eds.), *The Rome Statute of the International Criminal Court: A Commentary*, 3rd edition., C.H. Beck, Hart, Nomos, 2016, p. 322; ICC, *Situation in the Islamic Republic of Afghanistan*, Decision Pursuant to Article 15 of the Rome Statute on the Authorisation of an Investigation into the Situation in the Islamic Republic of Afghanistan, ICC-02/17, Pre-Trial Chamber II, 12 April 2019, para. 65 (excluding that the existence of a plan, policy or large-scale commission pursuant to Article 8(1) is a condition for the ICC to exercise its jurisdiction).

[29] See, e.g. International Criminal Court (ICC), Elements of Crimes, 2011 ("Elements of Crimes"), Article 8(2)(a)(i)(4) (international armed conflicts include situations of military occupation); Article 8 (2)(c)(i)-1(4).

[30] ICTY, *Prosecutor v. Dusko Tadić*, IT-94-1-AR72, Appeals Chamber, Decision, 2 October 1995, para. 70.

operations.[31] This definition has been endorsed by subsequent jurisprudence and international bodies,[32] including the ICC.[33]

In accordance with the definition provided, it is hence necessary to prove not only that an armed conflict existed at the time of the offence, but that the criminal conduct in question had a nexus with the hostilities. The question on whether IHL applies to cyber operations has been the object of intense debate, and at least three situations have been described: when the attack by cyber means is employed as part of an ongoing armed conflict; when it is conducted independently from other attacks; and when it is carried out extensively in conjunction with the use of conventional weapons, but the latter are on their own insufficient to qualify as an armed conflict.[34]

It is quite undisputed that IHL fully applies to cyber operations employed as 'force multipliers'[35] during existing conventional armed conflicts, i.e. when conducted in parallel or in addition to kinetic attacks directed against the adversary.[36] In such a case, however, in order to give rise to the applicability of IHL and consequently ensure the ICC jurisdiction, a nexus between the alleged offence perpetrated by cyber means and the armed conflict must be established. Article 8 of the Rome Statute indeed requires that the conduct be committed in the context of or in association with an already existing armed conflict.

Drawing from the ICTY's jurisprudence, it is necessary to prove that the offence is closely related to hostilities, in the sense that the armed conflict has played a prominent role in the perpetrator's ability and/or decision to commit such of-

---

31 The same set of rules also apply to situations of partial and total occupation, even if it is met with no armed resistance. See, Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 75 U.N.T.S. 31, Art. 2; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 75 U.N.T.S. 85, Art. 2; Geneva Convention Relative to the Treatment of Prisoners of War Aug. 12, 1949, 75 U.N.T.S. 135, Art. 2; Geneva Convention Relative to the Protection of Civilian Persons in Times of War, Aug. 12, 1949, 75 U.N.T.S. 287, Art. 2(2).

32 Sassòli, M.; Bouvier A.; Quintin A., *How Does Law Protect in Law, Cases; Documents and Teaching Materials on Contemporary Practice in International Humanitarian Law*, in Outline of International Humanitarian Law (3rd ed.) International Committee of the Red Cross, 2012, p. 22.

33 *Prosecutor v. Lubanga*, ICC-01/04-01/06, Trial Chamber, Judgment, 14 March 2012, para. 533.

34 Dinniss, H., *Cyber Warfare and the Laws of War*, Cambridge University Press, 2012, pp. 127-131.

35 Roscini, M., *Cyber Operations Can Constitute War Crimes Under the ICC Jurisdiction Without Need to Amend the Rome Statute*, ICC Forum, 2022, [https://iccforum.com/cyberwar#Roscini].

36 A well-known example is that of cyber operations conducted by alleged Russian hackers and targeting Georgian governmental and media websites in the framework of the 2008 international armed conflict between the Russian Federation and Georgia, which were unarguably subject to IHL applicable to IACs. Schmitt, M., *Cyber Operations and the Jus in Bello: Key Issues*, International Law Studies, Vol. 87, 2011, pp. 102-103. See, also: *ibidem*; Droege, *op. cit*, note 7, p. 542.

fence, in the way it was committed or the purposes for which it was committed.[37] The so-called *nexus requirement* has not been the object of extensive debate, as other issues have, especially considering the conventional international conflicts between States, where the actors participating in the hostilities were quite clearly defined. Conversely, as argued by Cottier, in contemporary NIACs, mixed or 'internalized' internal armed conflicts, "with often a wider array of different actors and less clear-cut front lines, the existence of a nexus frequently is less obvious".[38] Any prosecution of possible war crimes conducted by NSAs, who often operate transnationally, would therefore need to prove that the cyber operation had a link with the ongoing armed conflict. An indication of said link might be established by the fact that the victims belong to the adversary party, or that the action is undertaken in furtherance of the objectives of one party to the hostilities.[39] It must be noted that the assessment of the existence of a nexus with the armed conflict does not necessarily require a strict territorial link, provided that the nexus is otherwise established.[40]

The second hypothesis advanced acknowledges that not all cyber operations are performed in the framework of or in association with existing kinetic hostilities, but they may (and more often) consist in isolated computer network attacks carried out by States or NSAs[41] with (or without) repercussions in the kinetic world. In particular, it has been widely discussed whether cyber operations could amount to an armed conflict, and therefore trigger the applicability of IHL. In the scenario

---

37 The ICTY Trial Chamber held that, in determining whether an act is "sufficiently related to the armed conflict", the following factors can be taken into account: "the fact that the perpetrator is a combatant; the fact that the victim is a non-combatant; the fact that the victim is a member of the opposing party; the fact that the act may be said to serve the ultimate goal of a military campaign; and the fact that the crime is committed as part of or in the context of the perpetrator's official duties". Furtherly, the existence of an armed conflict need not be causal to the commission of the underlying crime, but it is required that such crime was committed because of the existence of a situation of armed conflict. ICTY, *Prosecutor v. Kunarac et al.,* IT-96-23 & IT-96-23/1-A, Appeals Chamber Judgment, 12 June 2002, paras. 58-60.

38 Cottier, *op. cit.*, note 28, p. 314 fn 56.

39 *See*, Schmitt, *op.cit.*, note 9, p. 392 (Rule 84 establishing the individual criminal responsibility for war crimes "does not apply to individuals engaged in purely criminal cyber operations or malicious cyber activities unrelated to the on-going international or non-international armed conflict").

40 One example is represented by the decision of the Appeals Chamber in the situation in the Islamic Republic of Afghanistan, which authorized an investigation on alleged war crimes and crimes against humanity related to the situation even when the alleged conduct occurred outside Afghan territory, and when the victims were captured outside of Afghanistan. *Situation in the Islamic Republic of Afghanistan*, ICC-02/17-138 OA4, Appeals Chamber, Judgment, 5 March 2020.

41 A famous example of an isolated computer network attack is the Stuxnet virus, introduced into the computers of two uranium facilities in the Islamic Republic of Iran at Natanz between 2009 and 2010. Droege, *op. cit.*, note 7, p. 542.

under consideration, our analysis being focused on the cyber activity of NSAs that may have the potential to negatively affect civilians or civilian infrastructure, it is worth considering whether and under which conditions such operations conducted outside the framework of armed conflict may autonomously amount to a NIAC. In determining whether cyber operations conducted in absence of kinetic armed conflict could amount to a NIAC, two criteria shall be considered: intensity and organization.[42]

Paragraphs (c)(d) and (e)(f) of Article 8 of the Rome Statute apply to NIACs and respectively cover serious violations of article 3 common to the four Geneva Conventions of 1949, when committed against persons who do not take active part in the hostilities, and other serious violations of the laws and customs applicable to conflicts not of an international character. The minimum level of intensity that the hostilities shall reach for IHL to apply slightly differ under the two sets of provisions of the Rome Statute covering NIACs.[43]

The minimum threshold required under Article 8 para. 2 (c) and (d) is the lowest one and is negatively defined by common article 3[44] excluding from the definition of NIACs "situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature".[45] This threshold hence typically requires some sort of continuity in the armed confron-

---

42 *Tadić*, *op. cit.*, note 30, para. 572.

43 It must be noted that under contemporary IHL at least three different regimes of 'minimum thresholds' can be distinguished: NIACs under common article 3, NIACs under Article 8(2)(e) and (f) of the Rome Statute of the ICC, and NIACs under Article 1 of Additional Protocol II, which is the highest threshold required and will not be addressed here. See, more accurately, Cottier, *op. cit.*, note 28, pp. 312-314.

44 In Article 8(2)(c) a certain number of guarantees for the "persons who do not take active part in the hostilities, including members of armed forces who have laid down their arms and those placed hors de combat by sickness, wounds, detention or any other cause" are set forth, and they include *inter alia* the prohibition of violence to life and person, the outrages against personal dignity, the taking of hostages, and the passing of sentences or carrying out of execution without appropriate judicial safeguards. Its application is regulated by subsequent paragraph (d), which states that paragraph (c) "applies to armed conflicts not of an international character and thus does not apply to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence or other acts of a similar nature". Rome Statute, Article 8(2)(c) and (d).

45 *Ibidem*, citing: Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) of 8 June 1977 (AP II), Article 1 para. 2. State practice has confirmed that the qualification of non-international armed conflicts as excluding situations of internal disturbances, riots, isolated and sporadic acts, and other acts of similar nature as provided in AP II is applicable to common Article 3 as well. See in this respect: ICRC Database, Treaties, States Parties and Commentaries, Convention (III) relative to the Treatment of Prisoners of War, Geneva, 12 August 1949, Commentary of 01.01.2020, Article 3 - Conflicts not of an international character, [https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/article-3/commentary/2020] Accessed 27 February 2023, paras. 420, 465.

tation between armed forces of a State and non-State armed groups, or among these groups.[46] In addition to the level of the armed violence, which shall not be sporadic, the armed groups involved must meet a certain degree of organization in order for the armed conflict threshold to be satisfied and IHL to be applicable, as is suggested by State practice and *opinio iuris*.[47]

The other threshold provided by Article 8 para. 2 (e) and (f) does not essentially differ from the threshold of common article 3. However, by reproducing the definition adopted by the AC in *Tadić*, these paragraphs are applicable when there is a *protracted* armed conflict between governmental authorities and organized armed groups or between such groups.[48] The term 'protracted' has been drawn from ICTY's jurisprudence as merely requiring some sort of duration of the hostilities, aimed at excluding civil unrest or terrorist activities from the ambit of the armed conflict.[49] ICC case-law seems to have excluded that the duration of the hostilities represents a distinct type of criteria envisaging a separate form of NIAC under paragraph (e). Conversely, when assessing the existence of a NIAC, the ICC's prosecution and Trial Chambers have considered exclusively the intensity of the armed conflict and the degree of the organization of the group, that should be sufficient to allow it to sustain protracted armed confrontations.[50]

In light of the above, in determining whether a NIAC involving cyber operations exists, the same criteria apply as for conventional armed violence.[51] Therefore, in order for a cyber operation conducted by NSA to fall within the ambit of article 8 para. 2 (c) to (f), it is necessary to prove that the operation reached a certain level of intensity and that the group satisfies a certain degree of organization. It appears reasonable to argue that only those operations that cause military harm to one of the belligerent parties, consisting for instance in physical damage to property, loss of life, injury to persons or significant disruption of critical infrastructure, could reach the intensity required to initiate a NIAC.[52] Indeed, with respects to the intensity criterion, isolated attacks conducted in absence of kinetic operations

---

46 Cottier, *op. cit.*, note 28, p. 313.

47 See, for instance, US Supreme Court, *Hamdan v. Rumsfeld*, 548 U.S. 65, 30 June 2006.

48 Rome Statute, Article 8(2)(f).

49 Cottier, *op. cit.*, note 28, p. 314; *Prosecutor v. Delalić.*, IT-96-21-T, Trial Chamber, Judgment, 16 November 1998, para. 184.

50 *See*, for instance, *Lubanga*, *op. cit.*, note 33, paras. 534-538; *Prosecutor v. Katanga*, ICC-01/04-01/07-3436-tENG, Trial Chamber, Judgment, 07 March 2014, paras. 1183-1187; *Prosecutor v. Bemba*, ICC-01/05-01/08-3343, Trial Chamber, Judgment, 21 March 2016, paras. 134-140. See, in general, ICRC *Commentary*, *op. cit.*, note 45.

51 Schmitt, *op.cit.*, note 9, pp. 385-391.

52 Dinniss, *op. cit.*, note 34, pp. 129-131; Roscini, *op. cit.*, note 35.

would be excluded from qualifying as a NIAC, even in cases where these attacks cause significant material harm and destruction, including loss of life.[53] It goes without saying that it is not likely that disruptive cyber operations that do not cause destruction would meet the criterion.[54] For instance, the Experts in the Tallinn Manual 2.0 exclude that "network intrusions, the deletion and destruction of data (even on a large scale), computer network exploitation, and data theft" amount to a NIAC, as would not mere blocking of functions and services, and defacing of websites.[55] However, among the Experts there was no consensus as to whether non-destructive cyber operations that are conducted during internal disturbances or alongside other acts of violence that alone are insufficient to qualify as a NIAC by organized armed groups could, however severe, be considered in order to fulfil the intensity criteria and trigger a NIAC.[56]

However, if we assume that a cyber operation fulfils the intensity criterion, the organization criterion would be even more difficult to prove in case of private individuals or loosely affiliated groups of hackers and online collectives. The organization of the parties involved in the hostilities, which has to be assessed on factual circumstances and determined on a case-by-case basis,[57] has been typically inferred from the existence of an effective command structure capable of coordinating military activities and determining a unified military strategy, as well as the group's capacity to conduct large-scale military operations.[58] Although online col-

---

53 See also Gisel, L., *et al.*, *op. cit.*, note 7, p. 305 ("while arguably not impossible in exceptional circumstances, it will be unlikely that cyber operations alone would meet the intensity requirement for a non-international armed conflict").

54 Schmitt, *op.cit.*, note 9, pp. 105-106; Dinniss, *op. cit.*, note 34, p. 131 (arguing that if an armed group launches a protracted series of attacks intended to cause physical damage to life and/or property, regardless of their kinetic or cyber nature, these acts would, under the ICRC interpretation, be considered the start of an armed conflict).

55 Schmitt, *op. cit.*, note 9, p. 388.

56 *Ibid*, p. 389. The view that cyber operations need to cause physical damage and injury, and to a certain extent potentially incapacitation, in order to reach the intensity level required by NIACs was also shared by the Council of Advisers in the Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare. See, The Permanent Mission of Liechtenstein to the United Nations, The Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare, 2021, [https://www.regierung.li/files/medienarchiv/The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf] Accessed February 2023.

57 *Prosecutor v. Limaj et al.*, IT-03-66-T, Trial Chamber, Judgment, 30 November 2005, para. 90 (in determining the organization of the Kosovo Liberation Army, the Trial Chamber considered for instance "factors including the existence of headquarters, designated zones of operation, and the ability to procure, transport, and distribute arms"). A group can be considered "armed", if it has the capacity to launch lethal or destructive cyber attacks. Schmitt, *op.cit.*, note 9, p. 389.

58 Conversely, it is not necessary that the group possesses a "conventional militarily disciplined unit". *See* Schmitt, *op.cit.*, note 9, p. 389; *Limaj*, TC Judgment, *op. cit.* 57, paras. 129-132.

lectives operating in cyberspace such as Anonymous appear to be driven by common causes and objectives, as in the case of the Russian/Ukrainian armed conflict when they shared forces against the Russian government, and their activities and targets are at least discussed among their members, their level of organization is questioned.[59] Their loose structure, the absence of a spokesperson or a chain of command, as well as of any sort of internal regulations or headquarters (these groups normally organize themselves online, and never meet)[60], would exclude that they are considered an organized armed group within the meaning of IHL.[61]

Of course, these considerations would not apply to armed groups with a sufficient degree of organization such as to enable them to implement and respect IHL and to carry out sustained and protracted attacks (both kinetic and cyber). In that case, IHL would apply and their members could be punishable for possible war crimes under the Rome Statute.[62] However, things would be different in case of armed groups with some degree of hierarchical structure, but who never met in person: in such a situation, the organization requirement would be difficult to prove.[63]

In conclusion both the intensity and the organization criteria would be challenging to meet in case of sporadic cyber operations by either private individuals or "hacktivist" groups, and IHL would not apply.[64] Conversely, their actions would be regulated by domestic criminal law and human rights law.[65]

---

59 Buchan, *op. cit.*, note 22, pp. 741-742.

60 Nevertheless, the majority of the Experts in the Tallinn Manual argue that the fact that these groups never met in person does not alone represent a ground to exclude altogether the organization requirement. Schmitt, *op.cit.*, note 9, p. 390.

61 On the organized armed group requirement, and the difficulty of applying it to digital groups, see for instance: Beatty G., *War crimes in cyberspace: prosecuting disruptive cyber operations under Article 8 of the Rome Statute*, The Military Law and the Law of War Review, Vol 58, No.2., 2020, p. 227. The majority of the Experts of the Tallinn Manual agreed that informal groups who operate "without any coordination" – i.e. without an informal leadership entity capable of directing the group's activities, identify potential targets, and maintaining an inventory of tools – would not satisfy the organization requirement, even if they shared a common goal. Schmitt, *op.cit.*, note 9, pp. 390-391.

62 Of course, in the case at hand, in order for the ICC to exert its jurisdiction, the other requisites shall also apply, i.e. the conduct shall fulfil the elements of Article 8 (both the mental and the material element), it shall be considered admissible under Article 17, and it shall take place in the territory of or by a national of a State party to the ICC Statute or a State that has accepted its jurisdiction.

63 The Experts in the Tallinn Manual were divided as to whether a "virtual armed group" would satisfy the organization requirement, "since there would be no means to implement the law with regard to individuals with whom there is no physical contact". Schmitt, *op. cit.*, note 9, p. 390.

64 Beatty, *op. cit.*, note 61, p. 227.

65 Schmitt, *op. cit.*, note 36, pp. 105-106.

3.2. The cyber operation must be sufficiently grave under Article 17 of the Rome Statute

Being the ICC a Court of last resort,[66] Article 17 of the Rome Statute imposes that in order for a case to be admissible, it must be "of sufficient gravity to justify further action by the Court".[67] Similarly, under Article 53, in deciding whether or not initiating an investigation or to proceed to a prosecution, the Prosecutor shall consider, *inter alia*, the gravity of the crime and the admissibility requirements under Article 17.[68]

Neither the Rome Statute nor its drafting history provide for criteria that should be used for the assessment of the gravity requirement.[69] The Office of the Prosecutor (OTP) and the Pre-Trial Chamber (PTC) have based their evaluation of the gravity requirement on two elements. On the one side, the gravity assessment included an evaluation of a series of factors, including the systematic nature of the conduct (i.e., the pattern of incidents), and the social alarm that the conduct(s) may have caused in the international community. On the other side, gravity has additionally been considered in light of the position of persons involved, including those who were the "most responsible" for the alleged systematic or large-scale commission of crimes.[70]

With respect to the first element, in the 2013 Policy Paper on Preliminary Examinations, the OTP has acknowledged that – provided that any crime that falls within the jurisdiction of the Court shall be serious in nature[71] – its assessment of

---

66 Contrary to the International *ad hoc* Criminal Tribunals for the Former Yugoslavia (ICTY) and for Rwanda (ICTR), which had primacy over domestic jurisdictions, the ICC shall be complementary with respect to national criminal jurisdiction and shall exercise its jurisdiction over cases when the State(s) that normally would have jurisdiction over it, is (are) unwilling or unable to carry out effective investigations or prosecutions. Rome Statute, Articles 1 and 17.

67 Rome Statute, Article 17(d).

68 Such evaluation must be done in the preliminary examinations under Article 53(1)(b), and during the investigations as a condition to begin the actual prosecution under Article 53(2)(b). Rome Statute, Article 53 para. 1(b)(c), para. 2(b)(c).

69 On the admissibility test pursuant to Article 17, see for instance: Werle, G.; Jeßberger, F., *Principles of International Criminal Law*, 4th Edition, Oxford University Press, Oxford, 2020, paras. 344-353. *See*, also, Roscini, M., *Gravity in the Statute of the International Criminal Court and Cyber Conduct That Constitutes, Instigates or Facilitates International Crimes*, Criminal Law Forum, Vol. 30, 2019, pp. 255 *et seq*.

70 *Prosecutor v. Lubanga,* ICC-01/04-01/06-1-Corr-Red, Decision on the Prosecutor's Application for a warrant of arrest, Article 58, 10 February 2006, paras 42 *et seq*.

71 See, Rome Statute, Preamble, Article 1, Article 5.

gravity includes both quantitative and qualitative considerations.[72] These include the scale, the nature, the manner of commission of the crimes, and their impact.

The scale refers to the number of victims, as well as to the harm imposed to them and to their families, to the extent of the damage or the geographical or temporal scale of crimes (the intensity might also be considered). In the interpretation of scale, the AC of the ICC clarified, however, that Article 8(1) does not impose a fixed requirement on war crimes to be part either of a plan or policy or of a large-scale commission to be admissible under Article 17.[73]

The nature of the crimes relates to specific elements of offences, which may be deemed of greater concern, for instance "killings, rapes and other crimes involving sexual or gender violence and crimes committed against children, persecution, or the imposition of conditions of life on a group calculated to bring about its destruction".[74]

The manner of commission considers for instance the existence of a plan or organized policy, the way the crimes were committed, or if they involved cruelty, as well as the vulnerability of the victims.[75]

Lastly, the terror or the sufferings inflicted on victims, as well as the social and environmental damage could be elements contributing to the impact as a factor to assess the gravity of a crime.[76]

Up until now, it does not seem that the cyber operations, especially when conducted by NSAs, have resulted in serious humanitarian consequences, their actions being limited to DDoS attacks or ransomwares. These "only result in temporary and reversible harm to the target" which "might lead to the temporary interruption of services but not physical damage of persons or property".[77] Therefore, to the current situation, it appears that it is unlikely that cyber operations conducted by NSAs would be grave enough to trigger the ICC's jurisdiction. According to Roscini, cyber operations could satisfy the gravity threshold if, for instance, they are characterized by cruelty (i.e. they may consist in a change in medical records,

---

72 ICC, Office of the Prosecutor, *Policy Paper on Preliminary Examinations*, November 2013, paras. 59 *et seq*.

73 ICC, *Situation in the Democratic Republic of the Congo*, ICC-01/04-169, Appeals Chamber, Judgment on the Prosecutor's appeal against the decision of Pre-Trial Chamber I entitled "Decision on the Prosecutor's Application for Warrants of Arrest, Article 58", 12 July 2006, paras. 70-71.

74 OTP, 2013 Policy Paper, *op. cit.*, note 72, para. 63.

75 *Ibid.*, para. 64.

76 *Ibid.*, para. 65.

77 Roscini, *op. cit.*, note 68, p. 263.

so that patients receive unnecessary treatment), or if they have significant impact or serious repercussions on national infrastructures, for instance by disrupting the provision of essential services to the population or causing damage to the natural environment, or if they target specially protected persons.[78]

With respect to the second element of gravity assessment relating to the persons involved, the Prosecutor and the PTC in the *Mavi Marmara* situation disagreed on how to identify those "most responsible" for the commission of the alleged crimes. By dismissing the position of the OTP, i.e. that the "most responsible" referred to senior military commanders and political leaders, the judges of the PTC argued that it rather referred to those persons who may "bear the greatest responsibility" for such crimes, regardless of their seniority or hierarchical positions.[79] In determining the individual criminal responsibility for cyber operations, the rank or other forms of leadership could be difficult to establish, or it "may give way to more horizontal structures and dynamics that depend more on cyber skills and (enemy) vulnerabilities than the capacity to command and control".[80] According to Roscini, individuals who operate in cyberspace may play different roles, which range from the material execution of the cyber attack, to the development of the malware used, or the recruitment and training of hack-

---

78 *Ibid.*, p. 266.

79 On 14 May 2013, the Government of the Union of the Comoros referred to the OTP a situation relating to an Israel raid on the Humanitarian Aid Flotilla bound for the Gaza strip. With a decision of 6 November 2014, the Prosecutor announced her decision not to investigate the incident and to close the preliminary examination, in particular on the grounds of insufficient gravity pursuant to articles 17(1)(d) and 53(1)(b) of the Statute. On 16 July 2015, following a request for the review of the decision by the Government, the PTC requested the OTP to reconsider the decision, by ruling that the Office erred in the assessment of gravity. On 6 November 2015, the Appeals Chamber, by majority, rejected the OTP's appeal against the decision of the PTC. After two years, on 29 November 2017, the Prosecutor reaffirmed her previous view that the information available did not provide a reasonable basis to proceed with an investigation. On 2 September 2019, the AC dismissed the Prosecutor's appeal against the decision of the PTC, which had ruled that she had to reconsider her decision. On 16 September 2020, the PTC rejected the Government's application for judicial review and decided not to request the Prosecutor to reconsider her decision. *Situation in The Registered Vessels of The Union of the Comoros, The Hellenic Republic and the Kingdom of Cambodia*, Decision on the request of the Union of the Comoros to review the Prosecutor's decision not to initiate an investigation, Pre-Trial Chamber I, ICC-01/13-34, 16 July 2015, paras. 23-24; Decision on the admissibility of the Prosecutor's appeal against the "Decision on the request of the Union of the Comoros to review the Prosecutor's decision not to initiate an investigation", Appeals Chamber, ICC-01/13 OA, 6 November 2015; Notice of Prosecutor's Final Decision under Rule 108(3), ICC-01/13, Pre-Trial Chamber, 29 November 2017; Judgment on the appeal of the Prosecutor against Pre-Trial Chamber I's 'Decision on the "Application for Judicial Review by the Government of the Union of the Comoros"', ICC-01/13 OA 2, 2 September 2019; Decision on the 'Application for Judicial Review by the Government of the Comoros', Pre-Trial Chamber I, ICC-01/13, 16 September 2020.

80 Saxon, D., *Violations of International Humanitarian Law by Non-State Actors during Cyberwarfare*, Journal of Conflict & Security Law, Vol. 21, No. 3, 2016, pp. 570-571.

ers, or provide the necessary information of a target. In these cases, they may be involved as co-perpetrators or accessories.[81] Moreover, individuals may also be criminally responsible for the employment of cyber operations used in order to instigate, aid, abet, or otherwise assist the commission of a crime carried out "traditionally" and be liable under Article 25(b)-(d) of the Rome Statute.[82] However, in the cyberspace scenario, which is characterized by anonymity, it may be extremely difficult to identify the "most responsible person" for the alleged commission of a crime.[83]

3.3. The cyber operation must fulfil the elements of war crimes under Article 8

When dealing with the application of the Rome Statute to cyber operations, IHL principles become of particular importance, namely those referring to distinction, proportionality, and precaution, as it is generally acknowledged that cyber operations specifically relate to targeting.

It is usually argued that only those cyber operations that amount to an "attack" within the meaning of Additional Protocol I can be subject to the application of IHL's principles and therefore constitute war crimes.[84] It is common ground that the notion of attack quite indisputably extends to those cyber operations "reasonably expected to cause injury or death to persons or damage or destruction to objects", but also serious illness and severe mental suffering equivalent to injury.[85] The causal effects are not limited to the direct consequences that an attack may cause on the targeted cyber system, but also include the consequential damage, destruction, injury or death that can be foreseen.[86] The example provided by the Experts in the Tallinn Manual includes the remote manipulation of a Supervisory Control and Data Acquisition (SCADA) system of a dam that results in the release of waters and consequential extensive downstream destruction and harm to individuals, without necessarily damaging the system itself.

---

81 Roscini, *op. cit.*, note 68, pp. 256-257.

82 Schmitt, *op.cit.*, note 9, pp. 395-396.

83 Roscini, *op. cit.*, note 68, p. 258.

84 Additional Protocol I, Article 49(1) (defining attacks as "acts of violence against the adversary, whether in offence or defence").

85 Schmitt, *op.cit.*, note 9, pp. 415 (also noting that "*de minimis* damage or destruction does not meet the threshold of harm required by [Rule 92]", and that "[n]on-violent operations, such as psychological cyber operations and cyber espionage, do not qualify as attacks"), p. 417.

86 *Ibid.*, p. 416.

Against this background, cyber attacks that target civilians[87] and civilian objects,[88] or that are indiscriminate in nature,[89] or that cause excessive incidental loss of life, injury or damage to civilians[90] are prohibited under IHL and may constitute war crimes.[91]

A more controversial issue is represented by cyber operations that do not result in physical damage, but that negatively affect the functionality of infrastructure. Although views differ, in general terms it may be argued that the interpretation of the notion of attack could also encompass those cyber operations that do cause a loss of function or which significantly disrupt a system, for instance by disabling a computer or a network, although they may not necessarily amount to a war crime.[92] The Experts in the Tallin Manual, for instance, were divided: while some of them excluded that mere interference with the functionality of an object amounts to damage or destruction, the majority argued that it does, to the extent that such interference with functionality requires a replacement of physical components, or reinstallation of the operating system or of particular data.[93] Moreover, according to the view of some of them, a cyber operation that manipulates, alters, or deletes specific data that cause a cyber infrastructure not to perform its intended functions, would amount to an attack as well.[94]

---

87 Pursuant to the principle of distinction, "[t]he civilian population as such, as well as individual civilians, shall not be the object of cyber attack". *Ibid.*, pp. 422-423.

88 *Ibid.*, pp. 434-435 ("Civilian objects shall not be made the object of cyber attacks. Cyber infrastructure may only be made the object of attack if it qualifies as a military objective").

89 *Ibid.*, pp. 455-457 ("It is prohibited to employ means or methods of warfare that are indiscriminate by nature", i.e., "(a) when they cannot be directed at a specific military objective, or (b) limited in their effects as required by the law of armed conflict and consequently are of a nature to strike military objectives and civilians or civilian objects without distinction").

90 Pursuant to the principle of proportionality, a "cyber attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated is prohibited". *Ibid.*, pp. 470-476.

91 *Ibid.*, p. 391.

92 The Council of Adviser adopts the view that Article 8's provisions deriving from IHL core principles only applies to "attacks" for the purposes of IHL, although underlining that neither the Elements of Crimes nor the ICC Statute do actually define them. Council of Advisers, *op. cit.*, note 56, pp. 37-39; Droege, *op. cit.*, note 7, p. 559 ("an attack must also be understood to encompass such operations that disrupt the functioning of objects without physical damage or destruction, even if the disruption is temporary"); Ambos, K., *International criminal responsibility in cyberspace*, in: Tsagourias, N.; Buchan, R. (eds.), Research Handbook on International Law and Cyberspace, 2015, p. 124 ("a cyber operation leaving the targeted object physically intact but neutralizing it in its functionality may amount to a militarily relevant attack, at least if the operation disables the 'critical infrastructure' of the respective State", footnotes omitted).

93 Schmitt, *op.cit.*, note 9, p. 417.

94 *Ibid.*, p. 418.

It is debated whether the deletion or alteration of data could be considered an attack even in absence of resulting damage or loss of functionality of the cyber infrastructure. Against the position of the Tallinn Manual on the issue (in which the majority of Experts excluded data from the category of objects protected under IHL due to their intangibility),[95] it is the opinion of several commentators that in view of the growing importance of data in digitized societies, civilian data are protected under IHL, and therefore their alteration and deletion could possibly be considered a violation of IHL, in particular when essential civilian data are involved.[96] Some authors indeed advocate for a progressive interpretation of the notion of "object" and "property" under the Rome Statute so as to include – under some conditions – certain categories of civilian data under the scope of protection offered by IHL, in light of the importance of protecting civilians and civilian objects from the effects of hostilities.[97]

On the other hand, it must be here also emphasized that it is the view of some commentators that disruptive cyber operations – i.e., those "actions that inter-

---

[95] There exists no definition of computer data under IHL instruments nor in the Rome Statute and States' practice on the issue is inconsistent. Scholars' views differ on whether to consider them as protected under IHL provisions, including in the Tallinn Manual, where not all Experts share the majority position that the notion of 'object' in international law of armed conflict shall not be interpreted as including data and that an attack on data *per se* does not constitute an attack under IHL. Instead, a minority of the Experts argues that data should be regarded as an object and protected from attack, in particular those which are deemed "essential to the well-being of the civilian population" such as "social security data, tax records, and bank accounts". Schmitt, *op.cit.*, note 9, p. 437.

[96] This "broader" view is also endorsed by the International Committee of the Red Cross, which considers 'essential civilian data' the "medical data, biometric data, social security data, tax records, bank accounts, companies' client files or election lists and records". ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, Policy paper, 28 November 2019 (ICRC 2019 Policy Paper), p. 8; Horowitz, J., *Cyber Operations under International Humanitarian Law: Perspectives from the ICRC*, American Society of International Law, Vol. 24, Issue 11, 2020, [https://www.asil.org/insights/volume/24/issue/11/cyber-operations-under-international-humanitarian-law-perspectives-icrc#_ednref16] Accessed August 2023. On the debate, see also Gisel *et al.*, *op. cit.*, note 7, p. 317 (noting that, since "data is an essential component of the digital domain and a cornerstone of life in many societies", the interpretation and application of "IHL rules to safeguard essential data against destruction, deletion or manipulation will be a litmus test for the adequacy of existing humanitarian law rules").

[97] It must be noted that data belonging to medical units are protected, in light of the specific protection granted by IHL to medical facilities and personnel. ICRC 2019 Policy Paper, *op. cit.*, note 96, p. 8; Schmitt, *op.cit.*, note 9, p. 515. On the debate relating to the interpretation of the notion of "object" under IHL as including data, see for instance, McKenzie, S., *Civilian Operations against Civilian Data*, Journal of International Criminal Justice, Vol. 19, 2021 (arguing that, when it comes to the conceptualization of data, "the more straightforward and protective option would be to recognize data as part of a physical system that is capable of being attacked" and advocating for a 'progressive' approach by the ICC, which "would be more protective of civilian and could encourage the progressive development of ICL and IHL"), pp. 1181 – 1182; Horowitz, *op. cit.*, note 96; Mačák, K., *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*, Israel Law Review, Vol. 48, No. 1, 2015, pp. 55 – 80.

rupt the flow of information or the functioning of information systems without causing physical damage or injury"[98] – may as well significantly affect the civilian population, for instance in the provision of essential services and in their access to basic need or they may undermine their fundamental human rights.[99]

Aside from the debate on what constitutes an "attack" in cyberwarfare, several offences listed in Art. 8 are indeed related to targeting and to the general prohibition on attacking particular protected targets, i.e. civilians[100] and civilian objects,[101] as well as personnel and objects involved in humanitarian assistance or peacekeeping missions or using distinctive emblems[102] or certain buildings or objects (e.g. dedicated to religion, education, art, science or charitable purposes, historic monuments, hospitals and places where the sick and wounded are collected), provided they are not military objectives.[103] There is broad consensus over the fact that cyber operations that are intentionally[104] directed against civilians and cause civilian casualties, which destroy protected objects, or which are expected to cause excessive incidental loss of life or injury to civilians or damage to civilian objects or the natural environment do fall within the purposes of Article 8,[105] and therefore entail the individual criminal responsibility of the perpetrator(s).

When considering the participation of NSAs in cyberwarfare and their individual criminal responsibility under the Rome Statute, there exist a few issues that ought to be discussed.

First, the expansion of the notion of object as encompassing data whose deletion restriction or tampering could result in injury or damage to civilian objects could

---

98 Brown, G.; Tullos, O., *On the Spectrum of Cyberspace Operations*, Small Wars Journal, 2012, p. 115.

99 One example provided is the 2017 WannaCry ransomware attack, which had a great impact on the UK's National Health Service, by shutting down computers, cancelling appointments, diverting ambulances and impacting emergency services. Beatty, *op. cit.*, note 61, p. 216. It must be noted that, even in cases that a cyber operation does "not result in the requisite harm to the object of the operation", if it "cause[s] collateral damage", then such operation might amount to an attack, according to the views of the Experts in the Tallinn Manual. Schmitt, *op. cit.*, note 9, pp. 418-419.

100 Rome Statute, Article 8(2)(b)(i), Article 8(2)(e)(i).

101 Rome Statute, Article 8(2)(b)(ii). The same offence is not provided for under NIACs.

102 Rome Statute, Article 8(2)(b)(iii), Rome Statute, Article 8(2)(b)(xxiv), Article 8(2)(e)(ii).

103 Rome Statute, Article 8(2)(b)(ix), Article 8(2)(e)(iii and iv).

104 The mental element required under the Rome Statute is regulated by Article 30, which requires intent in relation to the conduct, and knowledge in relation to the consequence or awareness that it will occur in the ordinary course of events. Recklessness or negligence are not accepted. On the general issue of the *mens rea* required under the ICC, see for instance: Finnin, S., *Mental Elements under Article 30 of the Rome Statute of the International Criminal Court: A Comparative Analysis*, International and Comparative Law Quarterly, Vol. 61, Issue 2, 2012, pp. 325-359.

105 Rome Statute, Article 8(2)(b)(iv).

not be considered as applying to NIACs, since – under the Rome Statute – there appears to be no analogous crime that protects civilian objects (which are not military objectives) from attack. This necessarily implies that even if the ICC adopted a broad interpretation of what constitutes an "object" under IHL, thus justifiably expanding the protection to civilian data, in an armed conflict between a State and an organized armed group, or between organized armed groups – provided that the pre-requisites for the existence of the armed conflict are satisfied – there would be no provision applicable to an attack deliberately directed against civilian data. Nonetheless, attacks against civilian objects are prohibited and criminalized under international customary law and therefore any State could potentially prosecute the alleged responsible of the conduct.[106]

Similarly, while Article 8(2)(e)(i) criminalizes the conduct of "intentionally directing attacks against the civilian population as such or against individual civilians not taking direct part in hostilities" even in NIACs, two additional provisions prohibiting disproportionate and indiscriminate attacks cannot be found as applying to NIACs under the Rome Statute. Even in this case, the ICC Statute lags behind international customary law, where indiscriminate[107] and disproportionate attacks[108] are prohibited and criminalized both in IACs and NIACs. This

[106] Henckaerts, J.; Doswald-Beck L., (eds.) *Customary International Humanitarian Law*, Vol. 1: Rules, Cambridge University Press, Cambridge, 2005 (ICRC Customary Law Study), Rule 7 ("The Statute of the International Criminal Court does not explicitly define attacks on civilian objects as a war crime in non-international armed conflicts. It does, however, define the destruction of the property of an adversary as a war crime unless such destruction be 'imperatively demanded by the necessities of the conflict'"). It must be noted that, during the Rome Conference, the customary status of the criminalization of the conduct of attacking civilian objects in NIACs appeared doubtful. However, it has been argued that the fact that a violation of the rule prohibiting attacks on civilian objects, when carried out with purposeful action, entails individual criminal responsibility can be deduced by the case-law of the ICTY. Werle; Jeßberger, *op. cit.*, note 69, paras. 1432-1433; *Prosecutor v. Kupreškić et al.*, IT-95-16-T, Trial Chamber Judgment, 14 January 2000, paras. 521 *et seq* (The protection of civilians in time of armed conflict, whether international or internal, is the bedrock of modern humanitarian law … Indeed, it is now a universally recognised principle, recently restated by the International Court of Justice [in the Nuclear Weapons case], that deliberate attacks on civilians or civilian objects are absolutely prohibited by international humanitarian law"; *Prosecutor v. Strugar*, IT-01-42-T, Trial Chamber, Judgment, 31 January 2005, paras. 224-226.

[107] *Ibid.*, Rule 11; *Tadić*, *op. cit.,* note 30, para. 134; *Prosecutor v. Kordić and Čerkez*, IT-95-14/2-PT, Trial Chamber, Decision on defence motion to dismiss the amended indictment for lack of jurisdiction based on the limited jurisdictional reach of articles 2 and 3, 2 March 1999, para. 31; *Kupreškić*, *ibid.*, para. 524.

[108] *Ibid.*, Rule 14. International customary law criminalizes the conduct of causing disproportionate incidental damage to civilians or civilian objects also in NIACs, as confirmed by State practice. Werle; Jeßberger, *op. cit.*, note 69, para. 1455; see also the Military manuals of Netherlands, Germany, Peru, Republic of Korea, Switzerland, available at ICRC Database, Customary IHL, *Practice relating to Rule 14, Proportionality in Attack*, [https://ihl-databases.icrc.org/en/customary-ihl/v2/rule14] Accessed 10 March 2023.

means that, even if it is proved beyond reasonable doubt that NSAs are involved in a NIAC (hence that the organization requirement and intensity threshold are satisfied) and they do conduct cyber operations that are indiscriminate or disproportionate, an amendment to the Rome Statute should be required to expand the same protection that is granted to the civilian population in IACs also to NIACs.

To conclude, it should be emphasized that cyber operations could satisfy the material element of other offences, in addition to those relating to targeting. For instance, it has been discussed that cyber attacks carried out against nuclear power plants with the required *mens rea* may result in wilful killing under Article 8 (2) paragraphs (a)(i) and (c)(i), or violence to life or serious injury to body or health under paragraphs (a)(iii) and (c)(i).[109] Other authors suggest that the provision prohibiting the intentional starvation of civilian as a method of warfare under the Rome Statute[110] could encompass some forms of disruptive cyber operations.[111] In this last case too, however, the protection of civilians from the deprivation of objects indispensable to their survival would only apply to IACs before the ICC, in absence of analogous provisions applicable to NIACs in the Rome Statute.

4. CONCLUDING REMARKS

The possibility that NSAs such as cyber-criminals, transnational criminal groups, terrorist organizations, loosely affiliated bands of hackers or even isolated individuals perpetrate cyber-operations entails multiple concerns for the safety of civilians and civilian infrastructure. The anonymity and de-territorialization that typically characterize cyberspace by nature do affect the participation of States and NSAs to hostilities without distinction. However, in the case of NSAs, as discussed above, a series of additional challenges and concerns must be considered, especially when dealing with the application of the Rome Statute to cyber operations. These relate to the same existence of an armed conflict, which would require a certain level of intensity and organization that – at the moment – would be difficult to reach. Moreover, against the views of some commentators, disruptive cyber operations that do not cause material harm or physical damage, or loss of life or injury seem to be excluded from the application of IHL. The conducts of NSAs in cyberspace

---

109 Chaumette, A., *International Criminal Responsibility of Individuals in Case of Cyberattacks,* International Criminal Law Review, Vol. 18, 2018, pp. 14 – 15.

110 Rome Statute, Article 8(2)(b)(xxv), prohibiting the conduct of "[i]ntentionally using starvation of civilians as a method of warfare by depriving them of objects indispensable to their survival, including wilfully impeding relief supplies as provided for under the Geneva Conventions" as a war crime applicable in IACs.

111 The author recalls that during negotiations non-food items such as medicines and blankets were mentioned as essential commodity or objects necessary to survival. Beatty, *op. cit.,* note 61, p. 234.

seem to be limited, for the moment, to DDoS attacks and ransomwares, which – absent a long-lasting tangible physical harm to persons or property – would hardly qualify as "attacks" under IHL nor would they trigger the ICC's jurisdiction.

However, it is imperative not to overlook or underestimate the potential cost of cyber operations conducted by NSAs and the grave consequences they may impose on civilians and civilian infrastructure. From this perspective, a comprehensive discussion regarding the application of ICC Statute provisions pertaining to war crimes must account for not only the challenges posed by conducts potentially amounting to war crimes in cyberspace but also, and with more difficulty, the involvement of NSAs in such operations and their individual criminal responsibility under international law. When faced with possible future examinations and investigations of situations and cases involving cyber operations, the ICC, and primarily the OTP and PTC should consider not only the admissibility issues, but also the statutory limits concerning war crimes. As things stand, Article 8 does not afford the same level of protection to civilians involved in NIACs as it does in IACs, especially those protecting civilian objects from attack or those protecting civilians from disproportionate and indiscriminate attacks. This could mean that, in the eventuality that the judges of the Court – if and when presented with conducts taking place in the cyberspace – adopted a broad interpretation of the notion of "object" so as to include data essential to the well-being of the civilian population, the same level of protection could not be afforded to civilians involved in NIACs.

Against this backdrop, whereas States could (and should) initiate proceedings against alleged perpetrators of war crimes by cyber means – namely in the cases where international customary law provides for a criminalization of the conducts discussed in the sections above and protects civilians and civilian objects, and provided domestic law is in line with international provisions –, States parties to the ICC should consider an amendment to the Rome Statute,[112] to limit the effects of hostilities on civilians as far as possible, regardless of the character of the armed conflict. More specifically, although the possibility of applying the Rome Statute provisions to cyber operations without needing to amend the Statute seem uncontested in legal doctrine, the absence of specific provisions prohibiting indiscriminate and disproportionate attacks, attacks against civilian objects, as well as the intentional starvation of civilians as a method of warfare as applying to NIACs necessarily limits the protection afforded to the civilian population from the adverse effects of hostilities.

[112] The amendment procedure of the Rome Statute is regulated by Articles 121 and 123 of the Rome Statute, under which any State Party may propose amendments also concerning the elements of crimes.

REFERENCES

BOOKS AND ARTICLES

1. Ambos, K., *International criminal responsibility in cyberspace*, in: Tsagourias, N.; Buchan, R. (eds.), Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, Cheltenham, 2015, pp. 118-143
2. Beatty G., *War crimes in cyberspace: prosecuting disruptive cyber operations under Article 8 of the Rome Statute*, The Military Law and the Law of War Review, Vol 58, No.2., 2020, pp. 209-239
3. Buchan, R., *Cyber Warfare and the Status of Anonymous under International Humanitarian Law*, Chinese Journal of International Law, 2016, Vol. 15, No. 4, pp. 741 – 772
4. Bussolati, N., *The Rise of Non-State Actors in Cyberwarfare*, in: Ohlin, J. D.; Govern, K.; Finklestein, C. (eds.), Cyberwar: Law and Ethics for Virtual Conflicts, Oxford University Press, 2015, pp. 102-126
5. Chaumette, A., *International Criminal Responsibility of Individuals in Case of Cyberattacks,* International Criminal Law Review, 2018, Vol. 18, pp. 1 – 35
6. Cottier, M., *Article 8, Part I: Introduction/General Remarks*, in: Triffterer O.; Ambos K. (eds.), The Rome Statute of the International Criminal Court: A Commentary, 3rd edition., C.H. Beck, Hart, Nomos, 2016
7. Dinniss, H., *Cyber Warfare and the Laws of War*, Cambridge University Press, 2012
8. Droege, C., *Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians,* International Review of the Red Cross, Vol. 94, No. 886, 2012, pp. 533 – 578
9. Ducheine, P. A. L.; Pijpers B. M. J., *The notion of cyber operations*, in: Tsagourias N., Buchan, R. (ed.), Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, Cheltenham, 2021, pp. 272-296
10. Finnin, S., *Mental Elements under Article 30 of the Rome Statute of the International Criminal Court: A Comparative Analysis*, International and Comparative Law Quarterly, Vol. 61, Issue 2, 2012, pp. 325 – 359
11. Gisel, L.; Rodenhäuser, T.; Dörmann, K., *Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts*, in: International Review of the Red Cross, 2020, Vol. 102, No. 913, pp. 287 – 334
12. Henckaerts, J.; Doswald-Beck L., (eds.) *Customary International Humanitarian Law*, Vol. 1: Rules, Cambridge University Press, Cambridge, 2005
13. Horowitz, J., *Cyber Operations under International Humanitarian Law: Perspectives from the ICRC*, American Society of International Law, Vol. 24, Issue 11
14. Lin, H., *Cyber conflict and international humanitarian law*, International Review of the Red Cross, Vol. 94, No. 886, 2012, pp. 515 – 531
15. Mačák, K., *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*, Israel Law Review, Vol. 48, No. 1, 2015, pp. 55 – 80
16. McKenzie, S., *Civilian Operations against Civilian Data*, Journal of International Criminal Justice, Vol. 19, 2021, pp. 1165 – 1192

17. Missiroli, A., *Present Tense: Cyber Defence Matters*, in: Pawlak, P; Delerue, F. (eds.), A Language of Power? Cyber Defence in the European Union, Chaillot Paper/176, November 2022
18. Roscini, M., *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford, 2014
19. Roscini, M., *Gravity in the Statute of the International Criminal Court and Cyber Conduct That Constitutes, Instigates or Facilitates International Crimes*, Criminal Law Forum, Vol. 30, 2019, pp. 247 – 272
20. Sassòli, M.; Bouvier, A.; Quintin, A., *How Does Law Protect in Law, Cases; Documents and Teaching Materials on Contemporary Practice in International Humanitarian Law*, in: Outline of International Humanitarian Law (3rd ed.), International Committee of the Red Cross, 2012
21. Saxon, D., *Violations of International Humanitarian Law by Non-State Actors during Cyberwarfare*, Journal of Conflict & Security Law, Winter 2016, Vol. 21, No. 3, pp. 555 – 574
22. Schmitt, M., *Cyber Operations and the Jus in Bello: Key Issues*, International Law Studies, Vol. 87., 2011, pp. 89 – 110
23. Schmitt, M. N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017
24. Stiano, A., *L'intervento di Anonymous nel conflitto tra Russia e Ucraina: Alcune riflessioni sullo* status *giuridico degli* hacker *attraverso il prisma del diritto internazionale umanitario*, Ordine internazionale e diritti umani, No. 4, 2022, pp. 982 – 1000
25. Werle, G.; Jeßberger, F., *Principles of International Criminal Law*, 4th Edition, Oxford University Press, Oxford, 2020

INTERNATIONAL CRIMINAL COURT

1. *Prosecutor v. Bemba*, ICC-01/05-01/08-3343, Trial Chamber, Judgment, 21 March 2016
2. *Prosecutor v. Katanga*, ICC-01/04-01/07-3436-tENG, Trial Chamber, Judgment, 07 March 2014
3. *Prosecutor v. Lubanga,* ICC-01/04-01/06-1-Corr-Red, Decision on the Prosecutor's Application for a warrant of arrest, Article 58, 10 February 2006
4. *Prosecutor v. Lubanga*, ICC-01/04-01/06, Trial Chamber, Judgment, 14 March 2012
5. *Situation in the Democratic Republic of the Congo*, ICC-01/04-169, Appeals Chamber, Judgment on the Prosecutor's appeal against the decision of Pre-Trial Chamber I entitled "Decision on the Prosecutor's Application for Warrants of Arrest, Article 58", 12 July 2006
6. *Situation in the Islamic Republic of Afghanistan*, ICC-02/17, Pre-Trial Chamber II, Decision Pursuant to Article 15 of the Rome Statute on the Authorisation of an Investigation into the Situation in the Islamic Republic of Afghanistan, 12 April 2019
7. *Situation in the Islamic Republic of Afghanistan*, ICC-02/17-138 OA4, Appeals Chamber, Judgment, 5 March 2020
8. *Situation in The Registered Vessels of The Union of the Comoros, The Hellenic Republic and the Kingdom of Cambodia*, ICC-01/13-34, Pre-Trial Chamber I, Decision on the request of the

Union of the Comoros to review the Prosecutor's decision not to initiate an investigation, 16 July 2015

9. *Situation in The Registered Vessels of The Union of the Comoros, The Hellenic Republic and the Kingdom of Cambodia,* ICC-01/13 OA, Appeals Chamber, Decision on the admissibility of the Prosecutor's appeal against the "Decision on the request of the Union of the Comoros to review the Prosecutor's decision not to initiate an investigation", 6 November 2015
10. *Situation in The Registered Vessels of The Union of the Comoros, The Hellenic Republic and the Kingdom of Cambodia,* ICC-01/13, Pre-Trial Chamber, Notice of Prosecutor's Final Decision under Rule 108(3), 29 November 2017
11. *Situation in The Registered Vessels of The Union of the Comoros, The Hellenic Republic and the Kingdom of Cambodia,* ICC-01/13 OA 2, Appeals Chamber, Judgment on the appeal of the Prosecutor against Pre-Trial Chamber I's 'Decision on the "Application for Judicial Review by the Government of the Union of the Comoros"', 2 September 2019
12. *Situation in The Registered Vessels of The Union of the Comoros, The Hellenic Republic and the Kingdom of Cambodia,* ICC-01/13, Pre-Trial Chamber I, Decision on the 'Application for Judicial Review by the Government of the Comoros', 16 September 2020

INTERNATIONAL CRIMINAL TRIBUNAL FOR THE FORMER YUGOSLAVIA

1. *Prosecutor v. Delalić.*, IT-96-21-T, Trial Chamber, Judgment, 16 November 1998
2. *Prosecutor v. Kordić and Čerkez*, IT-95-14/2-PT, Trial Chamber, Decision on defence motion to dismiss the amended indictment for lack of jurisdiction based on the limited jurisdictional reach of articles 2 and 3, 2 March 1999
3. *Prosecutor v. Kunarac et al.,* IT-96-23 & IT-96-23/1-A*,* Appeals Chamber, Judgment, 12 June 2002
4. *Prosecutor v. Kupreškić et al.*, IT-95-16-T, Trial Chamber Judgment, 14 January 2000
5. *Prosecutor v. Limaj et al.*, IT-03-66-T, Trial Chamber, Judgment, 30 November 2005
6. *Prosecutor v. Strugar*, IT-01-42-T, Trial Chamber, Judgment, 31 January 2005
7. *Prosecutor v. Tadić*, IT-94-1-AR72, Appeals Chamber, Decision, 2 October 1995

INTERNATIONAL DOCUMENTS

1. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 75 U.N.T.S. 31
2. Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 75 U.N.T.S. 85
3. Geneva Convention Relative to the Treatment of Prisoners of War Aug. 12, 1949, 75 U.N.T.S. 135
4. Geneva Convention Relative to the Protection of Civilian Persons in Times of War, Aug. 12, 1949, 75 U.N.T.S. 287
5. International Criminal Court, Elements of Crimes, 2011, ISBN No. 92-9227-232-2

6. Office of the Prosecutor, *Policy Paper on Preliminary Examinations*, Policy Paper, November 2013
7. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 U.N.T.S. 3
8. UN General Assembly, Rome Statute of the International Criminal Court (last amended 2010), 17 July 1998

LIST OF NATIONAL REGULATIONS, ACTS AND COURT DECISIONS

1. US Supreme Court, *Hamdan v. Rumsfeld*, 548 U.S. 65, 30 June 2006

REPORTS

1. Gisel L.; Olejnik, L. (eds.), *The potential human cost of cyber operations*, International Committee of the Red Cross, Report, 2018
2. International Committee of the Red Cross, *International Humanitarian Law and the challenges of contemporary armed conflicts - Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions*, Report, 2019
3. International Committee of the Red Cross, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, Policy paper, 2019

WEBSITE REFERENCES

1. Ambos, K., *Cyber-Attacks as International Crimes under the Rome Statute of the International Criminal Court?*, ICC Forum, 2022, [https://iccforum.com/cyberwar#Ambos], Accessed 20 February 2023
2. Brown, G., Tullos, O., *On the Spectrum of Cyberspace Operations*, Small Wars Journal, 2012, [https://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations], Accessed February 2023
3. Cerulus L., *Kyiv's hackers seize their wartime moment*, Politico, 2022, [https://www.politico.eu/article/kyiv-cyber-firm-state-backed-hacking-group/], Accessed November 2022
4. Costello, R. Á., *Facilitating the Use of Open Source Evidence at the International Criminal Court: Authentication and the Problem of Deepfakes*, ICC Forum, 2020, [https://iccforum.com/cyber-evidence#Costello], Accessed 15 November 2022
5. Goodin, D., After *Ukraine recruits an "IT Army," dozens of Russian sites go dark*, Arstechnica, 2022, [https://arstechnica.com/information-technology/2022/02/after-ukraine-recruits-an-it-army-dozens-of-russian-sites-go-dark/], Accessed November 2022
6. Holland, S., Pearson, J., *US, UK: Russia responsible for cyberattack against Ukrainian banks*, Reuters, 2022, [https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/], Accessed November 2022
7. ICRC Database, Treaties, States Parties and Commentaries, Convention (III) relative to the Treatment of Prisoners of War, Geneva, 12 August 1949, Commentary of 01.01.2020,

Article 3 - Conflicts not of an international character, [https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/article-3/commentary/2020], Accessed February 2023

8. ICRC Database, Customary IHL, Practice relating to Rule 14, Proportionality in Attack, [https://ihl-databases.icrc.org/en/customary-ihl/v2/rule14], Accessed 10 March 2023
9. Johnson, B., *Hackers Turn Conti Ransomware Against Russia as Twitter Suspends Some Anonymous Accounts*, HomelandSecurity Today, 2022, [https://www.hstoday.us/subject-matter-areas/cybersecurity/hackers-turn-conti-ransomware-against-russia-as-twitter-suspends-some-anonymous-accounts/], Accessed November 2022
10. Koloßa, S., *The Dangers of Hacktivism How Cyber Operations by Private Individuals May Amount to Warfare*, 2022, [https://voelkerrechtsblog.org/the-dangers-of-hacktivism/], Accessed 04 February 2023
11. Milmo, D., *Anonymous: the hacker collective that has declared cyberwar on Russia*, The Guardian, 2022, [https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia], Accessed November 2022
12. Roscini, M., *Cyber Operations Can Constitute War Crimes Under the ICC Jurisdiction Without Need to Amend the Rome Statute*, ICC Forum, 2022,, [https://iccforum.com/cyberwar#Roscini], Accessed November 2022
13. Schectman, J., Bing, C., *Ukraine calls on hacker underground to defend against Russia*, Reuters, 2022, [https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/], Accessed November 2022
14. Schmitt, M., N., Biggerstaff, W., C., *Ukraine Symposium – Are Civilians Reporting With Cell Phones Directly Participating In Hostilities?,* 2022, [https://lieber.westpoint.edu/civilians-reporting-cell-phones-direct-participation-hostilities/], Accessed 20 February 2023
15. Schmitt, M., N., *Ukraine Symposium – Using Cellphones To Gather and Transmit Military Information, A Postscript*, 2022, [https://lieber.westpoint.edu/civilians-using-cellphones-gather-transmit-military-information-postscript/], Accessed 20 February 2023
16. The Permanent Mission of Liechtenstein to the United Nations, *The Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare*, 2021, [https://www.regierung.li/files/medienarchiv/The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf], Accessed February 2023.
17. *To What Extent Can Cyber Evidence Repositories, and Digital and Open-Source Evidence, Facilitate the Work of the OTP, and the ICC More Generally?*, ICC Forum, 2020, [https://iccforum.com/cyber-evidence], Accessed 15 November 2022
18. *Who is Squad303 that is attacking Russia with Text Messages*, The Tech Outlook, 2022, [https://www.thetechoutlook.com/news/new-release/software-apps/who-is-squad303-that-is-attacking-russia-with-text-messages/], Accessed November 2022