Criminal Law Forum (2019) 30:247–272
https://doi.org/10.1007/s10609-019-09370-0

MARCO ROSCINI*

GRAVITY IN THE STATUTE OF THE INTERNATIONAL CRIMINAL COURT AND CYBER CONDUCT THAT CONSTITUTES, INSTIGATES OR FACILITATES INTERNATIONAL CRIMES

ABSTRACT. This article explores the application of the gravity threshold to cyber conduct that might fall under the jurisdiction of the International Criminal Court. It first looks at how international crimes within the jurisdiction of the Court can be committed, instigated or facilitated in and through cyberspace and then discusses the problems that might arise when assessing gravity in this context. In particular, the article applies the elements of the gravity assessment identified in the Court's case-law and by the Prosecutor, i.e. the identification of those "most responsible" for the alleged crimes and certain quantitative and qualitative factors, in order to determine the gravity of a case or situation involving cyber conduct.

I INTRODUCTION

The use of cyber technologies as a new means to commit, instigate or facilitate crimes under the International Criminal Court (ICC)'s jurisdiction has so far received little attention in international criminal law scholarship. Even the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, published by a group of experts in 2017, only devotes two rules (out of 154) to cyber international criminality.[1]

* Marco Roscini is Professor of Westminster Law School, University of Westminster. The author is grateful to Dr. Marco Longobardo and to the anonymous reviewers of this journal for their useful comments on previous versions of this article. The usual caveat applies. Contact e-mail: m.roscini@westminster.ac.uk

[1] See Rules 84 (Individual criminal responsibility for war crimes) and 85 (Criminal responsibility of commanders and superiors): Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), pp. 391, 396, respectively. For a recent in-depth assessment of the *Tallinn Manual*'s impact on state practice, see Dan Efrony and Yuval Shany, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations

With cyber crime continuing to increase in size, sophistication and cost every year, we have reached the tipping point where an examination of the repercussions on international criminal law of this unprecedented phenomenon has become necessary.[2]

This article explores one of the international criminal law issues raised by the use of cyber technologies, i.e. the application of the gravity threshold to situations and cases involving cyber conduct that constitutes, instigates or facilitates international crimes under the ICC jurisdiction. Indeed, as the Preamble of the Rome Statute affirms, the Court was established to investigate and prosecute only "the most serious crimes of concern to the international community as a whole",[3] while other crimes remain the domain of national jurisdictions. One of the mechanisms devised to ensure this division of labour is the inclusion in the ICC Statute of a threshold of sufficient gravity that a situation or case must cross for it to be admissible before the Court.[4] How does this threshold apply when it comes to criminal conduct in cyberspace?

In order to address this question, this article will proceed as follows. It will first briefly look at how international crimes within the jurisdiction of the ICC can be committed, instigated or facilitated in and through cyberspace and will then move to discuss the difficulties of assessing gravity in this context. In particular, the article will distinguish the two elements of the gravity assessment that, according to the Court, need to be taken into account in order to determine the gravity of a case or situation, i.e. the identification of those "most responsible" for the alleged crimes on the one hand and certain quantitative and qualitative factors on the other. Finally, it will examine the differences in the assessment of the "legal" and "relative" gravity of situations and cases involving cyber conduct that constitutes, instigates or facilitates international crimes.

Footnote 1 continued
and Subsequent State Practice", 112 *American Journal of International Law* (2018), pp. 583–657.

[2] On the definition of cyber crime, see Fausto Pocar, "Note sullo sviluppo della normativa internazionale sui crimini relativi ai sistemi di informazione", in *Studi in Onore di Umberto Leanza*, vol. I (Naples: Editoriale Scientifica, 2008), pp. 633–635.

[3] Preamble, Statute of the International Criminal Court, text in 2187 UNTS 3.

[4] According to the Special Rapporteur James Crawford, the inclusion of gravity as an admissibility threshold in the International Law Commission's 1994 draft Statute of the ICC had the purpose to avoid that the Court be "swamped by peripheral complaints involving minor offenders, possibly in situations where the major offenders were going free" (UN Doc. A/CN.4/SR.2330, para. 9).

II CYBER CONDUCT THAT MIGHT FALL UNDER THE ICC JURISDICTION

In spite of the fact that, by 1998, states had already started to address cyber criminality,[5] this issue was completely ignored during the negotiations of the Rome Statute and is therefore absent in the final version of the treaty. Conduct in cyberspace, however, might fall under the jurisdiction of the Court either because it constitutes a new means to commit a crime over which the ICC has jurisdiction under its Statute, or because it instigates or facilitates the commission of such a crime.[6]

As to the former aspect, cyber attacks conducted by the belligerents in the context of and associated with an armed conflict[7] which are, for instance, intentionally aimed at causing civilian casualties or at destroying protected objects, or which are known to result in "incidental loss of life or injury to civilians or damage to civilian objects or widespread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated", would amount to war crimes under Article 8(2)(b)(i), (ii) and (iv), and Article 8(2)(e)(i) of the Rome Statute. Indeed, cyber operations are

[5] In 2000, the UN General Assembly also called upon states to "ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies" (UN General Assembly Resolution 55/63, 4 December 2000, para. 1(a)). Furthermore, a number of treaties have been concluded to address cyber criminality. The 2001 Budapest Convention on Cybercrime, negotiated in the framework of the Council of Europe and entered into force on 1 July 2004, requires states parties to criminalize certain cyber offences in their domestic legislation, to extend their jurisdiction to offences originating from their territory or by their nationals, and to provide mutual assistance in investigations and prosecutions (the text of the Convention is in 41 *International Legal Materials* (2002), pp. 282 ff.). An Additional Protocol concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems was also adopted in 2003 and entered into force on 1 March 2006 (*ETS*, n. 189). See also the African Union Convention on Cyber Security and Personal Data Protection adopted on 27 June 2014 (text available at https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection).

[6] See Article 25(3) of the ICC Statute. If cyber crimes are considered new crimes and not new means to commit existing ones, on the other hand, their investigation or prosecution by the ICC would be impossible as in conflict with the *nullum crimen sine lege* principle (Article 22 of the ICC Statute).

[7] ICC, Elements of the Crimes (2011), Article 8 ff., pp. 13 ff., https://www.icc-cpi.int/nr/rdonlyres/336923d8-a6ad-40ec-ad7b-45bf9de73d56/0/elementsofcrimeseng.pdf.

able to produce damaging physical consequences in the analogue world by corrupting the operating systems of physical infrastructures such as Supervisory Control and Data Acquisition (SCADA) systems, which could result in the malfunction of such infrastructures and possible loss of life or destruction of property: the textbook example is a cyber attack conducted by a belligerent that shuts down the cooling system of a nuclear power reactor located in enemy territory, thus causing the release of radioactive substances that reach indiscriminately civilians. If accompanied by the required *dolus specialis*,[8] cyber attacks resulting in harmful physical consequences on individuals might also constitute acts of genocide (Article 6(a)), or, if they are "committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack", crimes against humanity (Article 7(1)(a) and (b)), whether or not they occur in the context of an armed conflict.

It is less likely, although not impossible, that a cyber attack could in itself amount to the crime of aggression. The relevant scenarios are those provided in Article 8 bis (2)(b) and (d) of the ICC Statute, which refer respectively to "the use of any weapons by a State against the territory of another State" and to "[a]n attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State".[9] Cyber tools and capabilities can indeed be used as a weapon to cause harm, and many national armed forces have now set up cyber units.[10] Article 8 bis (1), however, also requires that, to entail individual criminal liability, the act of aggression must be "by its character, gravity and scale … a *manifest* violation of the Charter of the United Nations".[11] This excludes minor uses of force and legally controversial ones: it is unlikely, therefore, that a cyber attack will be a *manifest* violation of the UN Charter because a) the scale of the effects might not be significant or known enough, or attribution

[8] According to Article 6 of the ICC Statute, an act of genocide requires an "intent to destroy, in whole or in part, a national, ethnical, racial or religious group, as such".

[9] Anne-Laure Chaumette, "International Criminal Responsibility of Individuals in Case of Cyberattacks", 18 *International Criminal Law Review* (2018), p. 8.

[10] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014), pp. 9–10, 50–52.

[11] Emphasis added.

might not be clear,[12] and b) there is still debate on if and when a cyber attack is a use of armed force (and *a fortiori* an act of aggression) and thus falls under the scope of the *jus ad bellum* provisions of the Charter.[13] It is not surprising, therefore, that, during the negotiations, some delegations expressed concern that, without an express reference, the text of Article 8 bis would not cover cyber attacks.[14]

Cyber technologies could also be used to instigate or facilitate the commission of crimes under the ICC jurisdiction. Accessory liability, for instance, could be engaged through an act preparatory of genocide like "a network intrusion to acquire the names of individuals registered as a certain race in a State census in order to engage in genocide".[15] Individuals could also incite others to commit genocide by posting comments to that aim on blogs, Twitter or other social media. In relation to the international crimes committed in the Kachin, Rakhine and Shan States since 2011, for instance, the International Independent Fact-Finding Mission on Myanmar established by the UN Human Rights Council noted the following:

> The role of social media is significant. Facebook has been a useful instrument for those seeking to spread hate, in a context where for most users Facebook *is* the Internet. Although improved in recent months, Facebook's response has been slow and ineffective. The extent to which Facebook posts and messages have led to real-world discrimination and violence must be independently and thoroughly examined.[16]

In September 2012, Azerbaijan also denounced cyber attacks conducted by a self-styled "Armenian Cyber Army" under the direction and control of Armenia that were "aimed at glorifying terrorists and insulting their victims, as well as at advocating, promoting and

[12] Marco Roscini, "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations", 50 *Texas International Law Journal* (2015), p. 233 ff.

[13] Kai Ambos, "Individual Criminal Responsibility for Cyber Aggression", 21 *Journal of Conflict and Security Law* (2016), p. 495.

[14] Assembly of States Parties to the Rome Statute of the International Criminal Court, Resumed sixth session, New York, 2–6 June 2008, Report of the Special Working Group on the Crime of Aggression, ICC-ASP/6/20/Add.1, p. 14.

[15] *Tallinn Manual 2.0*, *supra* note 1, p. 66.

[16] Report of the Independent International Fact-Finding Commission on Myanmar, UN Doc. A/HRC/39/64, 24 August 2018, para. 74.

inciting ethnically and religiously motivated hatred, discrimination and violence''.[17]

III GRAVITY IN THE ICC STATUTE

If it can hardly be doubted that, at least potentially, cyber conduct might constitute, instigate or facilitate an international crime, for the situation or case involving it to be admissible before the ICC it has to be of sufficient gravity. In the ICC Statute, gravity is first and foremost an element of the crimes: there are several references to gravity in the definition of crimes as contained in Articles, 6, 7, 8 and 8 bis.[18] As already mentioned, for instance, Article 8 bis (1) states that an act of aggression must be ''by its character, gravity and scale … a manifest violation of the Charter of the United Nations''.[19] Article 7 also provides that crimes against humanity must be ''committed as part of a widespread or systematic attack directed against the civilian population''. As to war crimes, Article 8(1) provides that the Court prosecutes them ''in particular when committed as part of a plan or policy or as part of a large-scale commission of such crimes''.[20] The Office of the Prosecutor (OTP) has acknowledged this ''as statutory guidance indicating that the Court should focus on war crimes meeting these requirements''.[21] The PTC, however, found that ''the

[17] Letter dated 6 September 2012 from the Chargé d'affaires a.i. of the Permanent Mission of Azerbaijan to the United Nations addressed to the Secretary-General, 7 September 2012, UN Doc. A/66/897–S/2012/687, p. 1.

[18] Article 5 also states that the Court's jurisdiction is limited to ''the most serious crimes of concern to the international community as a whole''. The elements of genocide and crimes against humanity imply that only grave conduct is envisaged (William A. Schabas, *An Introduction to the International Criminal Court* (5th ed., Cambridge: Cambridge University Press, 2017), p. 80; Margaret M. DeGuzman, ''Gravity and the Legitimacy of the International Criminal Court'', 32 *Fordham International Law Journal* (2009), p. 1407).

[19] Understanding 7, adopted at the 2010 Kampala Review Conference together with the definition of the crime aggression, explains that ''[n]o one component can be significant enough to satisfy the manifest standard by itself'' (Understandings regarding the amendments to the Rome Statute of the International Criminal Court on the Crime of Aggression, RC/Res.6, Annex III).

[20] Article 8(2)(a) also includes ''grave'' breaches of the 1949 Geneva Conventions on the Protection of Victims of War in the list of war crimes, while subparagraph (b), (c) and (e) refer to ''serious'' violations.

[21] Situation on Registered Vessels of Comoros, Greece and Cambodia, Article 53(1) Report, ICC-01/13-6-AnxA, 6 November 2014, para. 137.

term ''in particular'' in article 8(1) implies that the existence of a plan, policy or large-scale commission is not a condition for the Court's jurisdiction, contrary to what is provided for in article 7 with regard to crimes against humanity'' and that ''such a plan, policy or large-scale commission is unnecessary to establish the sufficient gravity in accordance with article 17(l)(d)''.[22]

Gravity, however, is also an admissibility threshold for the Court to have jurisdiction (''legal gravity''):[23] as Pre-Trial Chamber (PTC) I found, ''the fact that a case addresses one of the most serious crimes for the international community as a whole is not sufficient for it to be admissible before the Court''.[24] As is well known, Article 17(1)(d) of the ICC Statute provides that a case is inadmissible, and must then be rejected, if it ''is not of sufficient gravity to justify further action by the Court''. Article 53 also provides that the Prosecutor cannot initiate an investigation or, after an investigation, proceed to a prosecution if she considers the case inadmissible under Article 17.[25] Although both Articles 17 and 53 refer to ''cases'', the PTC found

[22] 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, Pre-Trial Chamber II, ICC-02/17, 12 April 2019, para. 65.

[23] The expressions ''legal'' and ''relative'' gravity are borrowed from Ignaz Stegmiller, *The Pre-Investigation Stage of the ICC. Criteria for Situation Selection* (Berlin: Duncker & Humblot, 2011), pp. 316, 425; and Kai Ambos, *Treatise on International Criminal Law*, Vol. III: International Criminal Procedure (Oxford: Oxford University Press, 2016), p. 292.

[24] Situation in the DRC, Decision on the Prosecutor's Application for Warrants of Arrest, Pre-Trial Chamber I, ICC-01/04-01/06-8-Corr, 10 February 2006, para. 41. See also Situation in Kenya, Decision Pursuant to Article 15 of the Rome Statute on the Authorization of an Investigation into the Situation in the Republic of Kenya, Pre-Trial Chamber II, ICC-01/09-19-Corr, 31 March 2010, para. 56; Situation in the Republic of Côte d'Ivoire, Corrigendum to ''Decision Pursuant to Article 15 of the Rome Statute on the Authorisation of an Investigation into the Situation in the Republic of Côte d'Ivoire'', Pre-Trial Chamber III, ICC-02/11-14-Corr, 15 November 2011, para. 201.

[25] The decision of the OTP not to initiate the investigation of situations because of insufficient gravity has so far occurred only twice: Iraq and *Mavi Marmara*, and only in the latter case was the decision challenged by the referring party (see OTP, Response to Communications Received Concerning Iraq, 9 February 2006, pp. 8–9, www.icc-cpi.int/Pages/item.aspx?name=otp-response-iraq-06-02-09; Situation on Registered Vessels of Comoros, Greece and Cambodia, Article 53(1) Report, *supra* note 21, paras. 133–148).

that these provisions also apply to situations.[26] When deciding whether to start the investigation of a situation, in particular, the Prosecutor needs to consider whether the *potential* cases likely to arise from it are sufficiently grave.[27] A potential case is defined ''by way of reference to: (i) the groups of persons involved that are likely to be the object of an investigation for the purpose of shaping the future case(s); and (ii) the crimes within the jurisdiction of the Court allegedly committed during the incidents that are likely to be the focus of an investigation for the purpose of shaping the future case(s)''.[28] In our context, therefore, the gravity assessment concerns both *situations* (also) involving potential cases related to criminal conduct in cyberspace, and *cases* against a person accused of such conduct.[29]

In addition to being an element of the crimes and a non-discretionary admissibility threshold, gravity also plays a third function in

[26] Situation in Kenya, Decision Pursuant to Article 15 of the Rome Statute, *supra* note 24, paras. 41–50. According to the PTC, ''[t]he gravity threshold provided for in article 17(1)(d) of the Statute must be applied at two different stages: (i) at the stage of initiation of the investigation of a situation, the relevant situation must meet such gravity threshold and (ii) once a case arises from the investigation of a situation, it must also meet the gravity threshold provided for in that provision'' (Situation in the DRC, Decision on the Prosecutor's Application for Warrants of Arrest, *supra* note 24, para. 45).

[27] Situation in Kenya, Decision Pursuant to Article 15 of the Rome, *supra* note 24, para. 58; Situation in Côte d'Ivoire, Corrigendum to ''Decision Pursuant to Article 15 of the Rome Statute'', *supra* note 24, para. 202; Situation in Georgia, Decision on the Prosecutor's request for authorization of an investigation, Pre-Trial Chamber I, ICC-01/15-12, 27 January 2016, para. 53; Situation in Burundi, Decision Pursuant to Article 15 of the Rome Statute on the Authorization of an Investigation into the Situation in the Republic of Burundi, Pre-Trial Chamber III, ICC-01/17-9-Red, 25 October 2017, para. 184. See also OTP, Policy Paper on Preliminary Examinations, November 2013, para. 59; Situation on Registered Vessels of Comoros, Greece and Cambodia, Article 53(1) Report, *supra* note 21, para. 134.

[28] Situation in Kenya, Decision Pursuant to Article 15 of the Rome, *supra* note 24, para. 59. See also Situation in Côte d'Ivoire, Corrigendum to ''Decision Pursuant to Article 15 of the Rome Statute'', *supra* note 24, para. 204.

[29] A crime is only an element of a case (Situation on 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-Anx, 16 July 2015, Partly Dissenting Opinion of Judge Peter Kovács, para. 24). See also Situation in Kenya, Decision Pursuant to Article 15 of the Rome, *supra* note 24, para. 65: a potential case for the purposes of assessing admissibility ''encompasses both crimes and one or several persons suspected to have committed those crimes in the course of specific incidents''.

the ICC framework, that of guiding the decision of the Prosecutor on the selection and prioritisation of *admissible* situations and cases to investigate and prosecute (''relative gravity'').[30] Relative gravity ''aims at focusing the Court's resources on the most serious available situations and, generally, on the most serious cases within each situation''.[31] Unlike in legal gravity, when it comes to selecting or prioritising situations and cases on the basis of relative gravity the Prosecutor enjoys broad discretion.[32]

There is nothing in the ICC Statute or its drafting history that sheds light on the factors to consider in order to assess the gravity of situations and cases under Articles 17 and 53. From the ICC case-law, however, it results that the gravity assessment is composed of two elements: an evaluation of whether the persons that are likely to be the object of the investigation or prosecution include those ''most responsible'' for the alleged crimes, and an assessment of both quantitative and qualitative factors, including the nature, scale, manner of commission and impact of the alleged crimes.[33] This two-

[30] Articles 53(1)(c) and 53(2)(c) of the ICC Statute. See deGuzman, *supra* note 18, p. 1405; Ignaz Stegmiller, ''The Gravity Threshold under the ICC Statute: Gravity Back and Forth in *Lubanga* and *Ntaganda*'', 9 *International Criminal Law Review* (2009), p. 562; Susana SáCouto and Katherine Cleary, ''The Gravity Threshold of the International Criminal Court'', 23 *American University International Law Review* (2008), pp. 850–854. Gravity also has a fourth function, that of guiding the Court in the determination of sentences (Article 78).

[31] Stegmiller, *supra* note 23, p. 356.

[32] SáCouto and Cleary, *supra* note 30, p. 854; Ambos, *supra* note 23, p. 293. In this context, transparency is of course important (deGuzman, *supra* note 18, p. 1465). A decision by the Prosecutor not to initiate an investigation can be reviewed by the PTC upon request of the referring party (member state or the Security Council) or, if the Prosecutor's decision is based exclusively on ''the interests of justice'', by the PTC *motu proprio* (Article 53(3)). In the former case, the PTC may only request the Prosecutor to reconsider its decision, while in the latter case the decision not to initiate investigations must be confirmed by the PTC.

[33] See Situation in Darfur, Sudan, Decision on the Confirmation of Charges, Pre-Trial Chamber I, ICC-02/05-02/09-243-Red, 8 February 2010, paras. 31–32; Situation in Kenya, Decision Pursuant to Article 15 of the Rome, *supra* note 24, paras. 59–62; Situation in the Republic of Côte d'Ivoire, Corrigendum to ''Decision Pursuant to Article 15 of the Rome Statute'', *supra* note 24, paras. 203–204; Situation in Georgia, Decision on the Prosecutor's Request for Authorization of an Investigation, *supra* note 27, para. 51; Situation in Burundi, Decision Pursuant to Article 15 of the Rome Statute, *supra* note 27, para. 184. Regulation 29(2) of the Regulations of the Office of the Prosecutor, adopted in 2009, also indicates that an evaluation of gravity must be made on the basis of both quantitative and qualitative factors, including, but not limited to, the scale, nature, manner of commission of the crimes,

pronged assessment will now be applied to conduct in cyberspace that constitutes, instigates or facilitates international crimes under the ICC jurisdiction.

IV "THOSE MOST RESPONSIBLE" FOR THE ALLEGED CRIMES

As to the first element of the gravity assessment, in the *Mavi Marmara* situation the Prosecutor and the PTC explicitly disagreed on the identification of the "most responsible person", or "those who bear the greatest responsibility", for the crimes allegedly committed. In particular, the OTP decided not to start an investigation because, inter alia, there was not "a reasonable basis to believe that 'senior IDF commanders and Israeli leaders' were responsible as perpetrators or planners":[34] the OTP, therefore, intended "most responsible" as referring to the "most senior" persons. If one applies this reasoning in the context of cyberspace, a case against a senior military commander who plans and orders multiple, damaging and unlawful cyber attacks would be considered graver than a case against a freelance hacker who, acting upon instructions, conducts the cyber attacks.[35] The problem is that rank and seniority could be difficult to establish in our context, as actors in cyberspace often operate not on the basis of hierarchical relationships but in "horizontal structures and dynamics that depend more on cyber skills and (enemy) vulnerabilities than the capacity to command and control".[36] In any case, the PTC rejected the OTP's reasoning because it limited the

---

Footnote 33 continued
as well as their impact (Regulations of the Office of the Prosecutor, ICC-BD/05-01-09, 23 April 2009, p. 17). See also OTP, 2013 Policy Paper on Preliminary Examinations, *supra* note 27, para. 66; Situation in Côte d'Ivoire, Request of Authorisation of an Investigation Pursuant to Article 15, ICC-02/11-3, 23 June 2011, para. 54; Situation on Registered Vessels of the Union of Comoros, Greece and Cambodia, Article 53(1) Report, *supra* note 21, para. 135.

[34] Prosecution Response to the Application for Review of its Determination under Article 53(1)(b) of the Rome Statute, ICC-01/13-14-Red, 30 March 2015, para. 62. The Prosecutor announced her decision not to investigate the *Mavi Marmara* incident in a sixty-one page report published in 2014 (Situation on Registered Vessels of Comoros, Greece and Cambodia, Article 53(1) Report, *supra* note 21).

[35] Dan Saxon, "Violations of International Humanitarian Law by Non-State Actors during Cyberwarfare: Challenges for Investigations and Prosecutions", 21 *Journal of Conflict and Security Law* (2016), p. 564.

[36] *Ibid.*, at 570–571.

jurisdiction of the Court only to certain categories of persons in conflict with the Statute,[37] and argued that the status of "most responsible persons" is not dependent on considerations of seniority or hierarchical position of those responsible for the alleged crimes.[38] For the PTC, "most responsible" rather refers to those who played the most significant role in the commission of the crime, whatever their position or rank.[39]

Individuals do play different roles in cyber operations: they could not only execute the payload and conduct the attacks, but also be involved as co-perpetrators and accessories when they develop and design the malware, recruit and train hackers, acquire the information on the targeted system necessary to conduct the attack, provide the hardware necessary to carry out the attack, and so on. Conduct in cyberspace might also be aimed at instigating, aiding, abetting or otherwise assisting the commission of traditional international crimes, for instance by hacking into a system in order to obtain classified information necessary to enable the international crime to be committed, or by "posting online exhortations to continue the slaughter of civilians of a particular religious group during an armed conflict".[40] It is worth recalling that, in many legal systems, the

[37] The Preamble of the Statute affirms that the parties intended "to put an end to impunity for the perpetrators" of the crimes, not only for the most senior leaders, and Article 27(1) provides that the ICC Statute "shall apply equally to all persons without any distinction based on official capacity" (Situation in the DRC, 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", Appeals Chamber, ICC-01/04-169, 13 July 2006, paras. 78–79).

[38] Situation on 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, *supra* note 29, para. 23. See also Situation in the DRC, Judgment on the Prosecutor's Appeal, *supra* note 37, paras. 73–75. In relation to the crime of aggression, however, Article 8 bis (1) of the ICC Statute limits the jurisdiction of the Court only to senior leaders, i.e. those "in a position effectively to exercise control over or to direct the political or military action of a State".

[39] In the decision on Burundi, however, the PTC noted that "[i]n view of the Prosecutor's assertion that high-ranking officials of the Burundian government, the police, the intelligence service and the military services, but also the *Imbonerakure*, appear to be the most responsible for the most serious crimes, the Chamber accepts that the persons likely to be the focus of an investigation for the purpose of shaping a future case or cases are those who may bear the greatest responsibility for the alleged crimes" (Situation in Burundi, Decision Pursuant to Article 15 of the Rome Statute, *supra* note 27, para. 187).

[40] *Tallinn Manual 2.0*, *supra* note 1, pp. 395–396.

responsibility of accomplices or accessories is regarded as less grave than that of those who commit the crimes.[41]

The problem with the application of the ''most responsible'' factor in our context is that it might be difficult to obtain sufficient evidence of attribution of the conduct, particularly at the preliminary examination stage. It is well known that anonymity is one of the main characteristics of cyberspace. The internet, in particular, is a decentralized system where the communications protocol divides the sent data into several packets that take different unpredictable pathways to reach their destination before being reassembled.[42] An IP address identifies the origin and the destination of the data: with the cooperation of the Internet Service Provider (ISP) through which the system corresponding to the IP address is connected to the internet, it could be associated with a person, group or state. The IP address, however, could have been ''spoofed'', or the corresponding computer system may only be a ''stepping stone'' for an attacker located elsewhere.[43] Providing sufficient evidence of the identity of the hacker so to determine whether he/she is the ''most responsible person'', then, might be a challenging task for the Prosecutor and will require the cooperation of the states from which the cyber operation was conducted.[44] In 2013, the Office of the Prosecutor hired an expert in

[41] *Tallinn Manual 2.0*, *supra* note 1, p. 395.

[42] As has been observed, ''the internet is one big masquerade ball. You can hide behind aliases, you can hide behind proxy servers, and you can surreptitiously enslave other computers to do your dirty work'' (Joel Brenner, *America The Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011), p. 32).

[43] Scott J. Shackelford and Richard B. Andres, ''State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem'', 42 *Georgetown Journal of International Law* (2011), p. 982. The 1998 ''Solar Sunrise'' attack that broke into the US Department of Defense's system, for instance, was carried out by an Israeli teenager and Californian students through a computer based in the United Arab Emirates (Scott J. Shackelford, ''From Nuclear War to Net War: Analogizing Cyber Attacks in International Law'', 27 *Berkeley Journal of International Law* (2009) 192, p. 204).

[44] The 2015 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security established by the UN General Assembly, for instance, recommends that ''States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs [information and communication technologies] and implement other cooperative measures to address such threats'' (UN Doc. A/70/174 (2015), para. 13(d)).

digital forensics for its Scientific Response Unit to improve its ability to collect and analyse digital evidence.[45]

Having said that, at the preliminary stage the standard of proof is not "beyond reasonable doubt", a standard which is only necessary for convictions:[46] it suffices that there is a "reasonable basis to proceed", as there is still no accused to protect and the Prosecutor acts only on the basis of publicly available information.[47] The evaluation of admissibility, including gravity, is however stricter at the post-investigation stage and the lack of sufficient evidence might be a significant obstacle for the identification and prosecution of those "most responsible" for the crimes involving conduct in cyberspace.[48]

---

[45] Human Rights Center, "Digital Fingerprints. Using Electronic Evidence to Advance Prosecutions at the International Criminal Court", February 2014, p. 5, https://www.law.berkeley.edu/files/HRC/Digital_fingerprints_interior_cover2.pdf. On the use of digital evidence in ICC proceedings, see Eya David Macauley, "The Use of EO Technologies in Court by the Office of the Prosecutor of the International Criminal Court", in Ray Purdy and Denise Leung (eds.), *Evidence from Earth Observation Satellites. Emerging Legal Issues* (Leiden: Nijhoff, 2013), pp. 217–240; Aida Ashouri, Caleb Bowers and Cherrie Warden, "The 2013 Salzburg Workshop on Cyber Investigations: An Overview of the Use of Digital Evidence in International Criminal Courts", 11 *Digital Evidence and Electronic Signature Law Review* (2014), p. 115.

[46] Article 66(3) of the ICC Statute.

[47] Article 53(1). See Megumi Ochi, "Gravity Threshold before the International Criminal Court: An Overview of the Court's Practice", ICD Brief, 19, January 2016, p. 15. It is worth recalling that, in contrast with the OTP, the PTC argued that "if … the events are unclear and conflicting accounts exist, this fact alone calls for an investigation rather than the opposite. It is only upon investigation that it may be determined how the events unfolded" (Situation on 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, *supra* note 29, para. 36). For the PTC, in other words, uncertainty favours investigations rather than the opposite. Therefore, the investigations should be started even in the presence of insufficient or contradictory information about the gravity admissibility threshold. This conclusion has met with considerable criticism, including by the dissenting judge (Partly Dissenting Opinion of Judge Péter Kovács, *supra* note 29, paras. 6–12), as it would require the Prosecutor "to open an investigation whenever there exists a scintilla of evidence, no matter how persuasive, that might possibly satisfy the requirements of Article 53(1)" (Alex Whiting, "The ICC Prosecutor should Reject Judges' Decision in Mavi Marmara", Just Security, 20 July 2015, https://www.justsecurity.org/24778/icc-prosecutor-reject-judges-decision-mavi-marmara).

[48] Article 53(2) requires that there be a "sufficient basis" for prosecution, which is arguably a higher standard than "reasonable basis to proceed" (Marco Longobardo, "Everything is Relative, Even Gravity", 14 *Journal of International Criminal Justice* (2016), pp. 1022–1023).

V THE QUANTITATIVE AND QUALITATIVE ELEMENTS OF THE GRAVITY ASSESSMENT

As to the second aspect of the gravity assessment, the ICC case-law has indicated that an evaluation of gravity must be made on the basis of both quantitative and qualitative factors, including, but not limited to, the scale, nature, manner of commission of the crimes, as well as their impact.[49] These factors have been applied by the OTP and the PTC to assess the gravity of both situations and cases. They were for instance applied by the Prosecutor in her decision not to start investigations on the *Mavi Marmara* incident because of insufficient gravity.[50] The PTC found that the factors used by the Prosecutor were appropriate, but it concluded that they were applied incorrectly.[51]

The next pages will discuss how the qualitative and quantitative factors identified by the OTP and the Court may affect the assessment of the gravity of situations and cases involving cyber conduct that constitutes, instigates or facilitates international crimes under the ICC jurisdiction. It is worth recalling that these factors do not have a fixed weight and must be assessed in the light of the circumstances of each case.[52] Also, it is not essential that *all* conditions are satified, providing that "the overall assessment demonstrates sufficient gravity".[53]

5.1 *Scale*

Scale includes, among others, "the number of direct and indirect victims, the extent of the damage caused by the crimes, in particular the bodily or psychological harm caused to the victims and their families, or their geographical or temporal spread (high intensity of

[49] See *supra*, note 33.

[50] Situation on Registered Vessels of Comoros, Greece and Cambodia, Article 53(1) Report, *supra* note 21, para. 138 ff. See the critical comments of Russell Buchan, "The *Mavi Marmara* Incident and the International Criminal Court", 25 *Criminal Law Forum* (2016), pp. 497–498.

[51] Situation on 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, *supra* note 29, paras. 20–21.

[52] William A. Schabas, "Prosecutorial Discretion *v.* Judicial Activism at the International Criminal Court", 6 *Journal of International Criminal Justice* (2008), p. 740.

[53] Melanie O'Brien, "Prosecutorial Discretion as an Obstacle to Prosecution of United Nations Peacekeepers by the International Criminal Court", 10 *Journal of International Criminal Justice* (2012), p. 543.

the crimes over a brief period or low intensity of crimes over an extended period)''.[54] On this basis, for instance, the OTP decided not to open an investigation on the *Mavi Marmara* attack as the number of victims was ''relatively limited'' compared to other cases investigated by the Prosecutor.[55] The number of victims has also been considered important by the PTC, for instance in its decisions to authorise investigations in the situations in Kenya and Georgia.[56]

As noted in Section II, it is not doubted that cyber attacks could potentially cause significant physical damage to persons and objects. One could think of a cyber attack that shuts down an electrical power station in the middle of a harsh winter with consequent deaths among the civilian population due to the low temperatures, or a cyber attack that incapacitates computers controlling waterworks and dams, thus generating floodings of inhabited areas, or that disables the air traffic control system with consequent downing of civilian aircraft.[57]

It should be pointed out that cyber attacks can produce multiple effects in the physical world.[58] The primary effects are those on the attacked computer system or network, i.e. the deletion, corruption, or alteration of data or software, or system disruption through a Distributed Denial of Service (DDoS) attack or other cyber attacks.[59]

[54] OTP, 2013 Policy Paper on Preliminary Examinations, *supra* note 27, para. 62.

[55] Situation on Registered Vessels of Comoros, Greece and Cambodia, Article 53(1) Report, *supra* note 21, para. 138.

[56] See Situation in Kenya, Decision Pursuant to Article 15 of the Rome, *supra* note 24, paras. 190–191; Situation in Georgia, Decision on the Prosecutor's Request for Authorization of an Investigation, *supra* note 27, para. 5.

[57] Some of these examples are made in the UK Attorney General's speech at Chatham House, ''Cyber and International Law in the 21st Century'', 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

[58] William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington: The National Academies Press, 2009), p. 80. See also Pia Palojärvi, *A Battle in Bits and Bytes: Computer Network Attacks and the Law of Armed Conflict* (Helsinki: Erik Castrén Institute of International Law, 2009), p. 32; William H. Boothby, ''Methods and Means of Cyber Warfare'', 89 *International Law Studies* (2013), p. 390.

[59] Denial of service (DoS) attacks do not normally penetrate into the target system but inundate it with excessive messages or requests in order to overload it and force its shut down. Permanent DoS attacks are particularly serious attacks that damage the system and cause its replacement or reinstallation of hardware. When the DoS attack is carried out by a large number of computers organized in botnets, it is referred to as a ''distributed denial of service'' (DDoS) attack.

The secondary effects are those on the infrastructure operated by the attacked system or network (if any), i.e. its partial or total destruction or incapacitation. Tertiary effects are those on the owners of the systems which are staging the cyber operation, for example the owners of botnet-infected computers or of staging servers for exfiltration of stolen data, and on the users of the attacked system or infrastructure, for instance those persons that benefit from the electricity produced by a power plant disabled by a cyber operation.[60] Physical damage to property, loss of life and injury of persons, then, are the secondary or tertiary effects of a cyber operation, not the primary ones.

Scale includes not only the number of victims, but also an assessment of geographical and temporal spread. Cyber operations, however, might have a significant geographical spread but still result in limited physical damage. The malicious worm Stuxnet, for instance, spread to computers across several countries, including Iran, Indonesia, India, Azerbaijan, United States and Pakistan, but only allegedly caused physical damage to the Iranian uranium enrichment facility in Natanz, while causing little harm to computers that did not meet certain specific characteristics.[61] DDoS attacks also often in-

[60] These effects can be permanent (if the operation results in data loss or physical damage), temporary (if data recovery is possible and functionality can be restored), or transient (when normal functioning resumes immediately after the end of the attack through rebooting or resetting the system). See Robert Fanelli and Gregory Conti, ''A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict'', Christian in Czosseck, Rain Ottis, and Katharina Ziolkowski (eds.), *2012 4th International Conference* on Cyber Conflict (CCDCOE, 2012), pp. 323–4.

[61] In September 2010, it was reported that a computer worm, dubbed Stuxnet, had attacked Iran's industrial infrastructure with the alleged ultimate purpose of sabotaging the gas centrifuges at the Natanz uranium enrichment facility, one of the sites where the Islamic Republic is developing a nuclear programme (Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier,* version 1.4, February 2011 www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf). Even though an earlier version had already been released as early as 2007, the worm– which presumably infiltrated the Natanz system through laptops and USB drives, since it is not usually connected to the internet for security reasons – mainly operated in three waves between June 2009 and May 2010. Stuxnet had two components: one designed to force a change in the centrifuges' rotor speed, inducing excessive vibrations or distortions, and one that recorded the normal operations of the plant and then sent them back to plant operators so to make it look as everything was functioning normally (William J. Broad, John Markoff and David E. Sanger, ''Israeli Test on Worm Called Crucial in Iran Nuclear Delay'', *The New York Times*, 15 January 2011, https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html).

volve millions of botnets across several countries hijacked by a botmaster, but they only cause temporary and reversible harm to the target by shutting down the servers and systems overflooded with requests: this might lead to the temporary interruption of services, but not physical damage to persons or property. It is unlikely, therefore, that, even assuming for the sake of argument that they amounted to crimes under the jurisdiction of the Court, operations like the 2007 DDoS attacks on Estonia, which disrupted banking and communications infrastructures in the Baltic country, would be considered grave from a scale point of view in spite of their geographical spread, unless they also resulted in loss of life or destruction of physical property.[62]

Be that as it may, the ICC Appeals Chamber found that the conduct does not have to be "systematic or large scale" to cross the gravity admissibility threshold, as this would introduce "at the admissibility stage of proceedings criteria that effectively blur the distinction between the jurisdictional requirements for war crimes and crimes against humanity that were adopted when defining the

---

Footnote 61 continued
Although the exact consequences of the incident are still the object of debate, the International Atomic Energy Agency (IAEA) reported that Iran stopped feeding uranium into a significant number of gas centrifuges at Natanz (William J. Broad, "Report Suggests Problems with Iran's Nuclear Effort", *The New York Times*, 23 November 2010, www.nytimes.com/2010/11/24/world/middleeast/24nuke.html). While the worm was promiscuous, it made itself inert if the specific Siemens software used at Iran's Natanz enrichment plant was not found on infected computers, and contained safeguards to prevent each infected computer from spreading the worm to more than three others. The worm was also programmed to erase itself on 24 June 2012 (Jeremy Richmond, "Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?" 35 *Fordham International Law Journal* (2011–2012), p. 856).

[62] In 2007, a three week DDoS attack targeted Estonia, one of the most wired countries in the world, shutting down government websites first and then extending to newspapers, TV stations, banks, and other targets (Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents. Legal Considerations* (CCDCOE, 2010), pp. 18 ff., https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf). The attack, which, at least in its second phase, involved more than one million computers based in over 100 countries hijacked and linked through the use of botnets, followed the decision of the Estonian government to remove a Soviet war memorial from Tallinn city centre and, overall, lasted almost a month. The attack caused some limited economic and communication disruption, but no material damage, injuries, or loss of life (Sean M. Watts, "Low-Intensity Computer Network Attack and Self-Defense", 87 *International Law Studies* (2011), p. 70). Websites were also defaced and their content replaced with pro-Russia propaganda.

crimes that fall within the jurisdiction of the Court".[63] The Appeals Chamber also noted that a requirement for "large scale and systematic" conduct in the context of Article 17(1)(d) of the ICC Statute "would not only render inutile article 8 (1) of the Statute contrary to the principles of interpretation but would further contradict the express intent of the drafters in rejecting any such fixed requirement therein".[64]

5.2 *Nature*

It is not essential, however, that a situation or case involves an extensive number of casualties in order to justify investigation and prosecution.[65] Indeed, qualitative factors need also to be taken into account. Nature "refers to the specific elements of each offence such as 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".[66] This implies that certain crimes are by definition graver than others: for instance, national and international sources suggest that murder is considered the most serious crime from a sentencing point of view.[67] Crimes of sexual violence and those involving torture and physical/psychological suffering are also considered serious, while – as recalled by the Trial Chamber[68] – crimes against property are considered comparatively less serious.[69] The argument according to which there is a hierarchy among crimes

[63] Situation in the DRC, Judgment on the Prosecutor's Appeal, *supra* note 37, para. 70.

[64] *Ibid.*, para. 71.

[65] Situation in Burundi, Decision Pursuant to Article 15 of the Rome Statute, *supra* note 27, para. 184. O'Brien argues that it is "essential to prosecute perpetrators of mass atrocities that result in a comparatively "low" number of victims … as a deterrent but also to demonstrate that such conduct is unacceptable to the international community" (O'Brien, *supra* note 53, p. 544).

[66] OTP, 2013 Policy Paper on Preliminary Examinations, *supra* note 27, para. 63.

[67] DeGuzman, *supra* note 18, p. 1452.

[68] Situation in Mali, Judgment and Sentence, Trial Chamber VIII, ICC-01/12-01/15-171, 27 September 2016, para. 77.

[69] Situation in Mali, Judgment and Sentence, Trial Chamber VIII, ICC-01/12-01/15-171, 27 September 2016, para. 77. See DeGuzman, *supra* note 18, p. 1452; Kevin Jon Heller, "Situational Gravity Under the Rome Statute", in Carsten Stahn and Larissa van den Herik (eds.), *Future Perspectives in International Criminal Justice* (The Hague: T.M.C. Asser Press, 2010), p. 230.

within the jurisdiction of the Court, and war crimes in particular, is controversial, as it does not find an explicit basis in the letter of the Statute.[70] If it is accepted, however, cases involving cyber attacks that only cause damage to physical property (like the case of Stuxnet) might not be considered grave enough by their nature especially if compared to other cases involving killing or physical suffering. As will be seen, this argument seems more appropriate for the assessment of gravity in the selection and prioritisation of admissible cases by the OTP rather than for gravity as an admissibility threshold.[71]

Individuals might be responsible not only for acts, but also for omissive conduct in cyberspace, particularly in the case of superior or command responsibility for failure to prevent or repress a cyber operation constituting, instigating or facilitating an international crime conducted by someone under their effective control (Article 28 of the Rome Statute): in the *Ali* decision, the PTC considered untenable the defence's argument that a case concerning omissions could never be of sufficient gravity, as such conclusion is inconsistent with the letter, object and purpose of the Statute.[72]

5.3 *Manner of Commission*

Criteria to assess this factor include, inter alia, "the means employed to execute the crime, the degree of participation and intent of the perpetrator (if discernible at this stage), the extent to which the crimes were systematic or result from a plan or organised policy or otherwise

---

[70] Schabas, *supra* note 18, p. 81; Stegmiller, *supra* note 23, p. 352; Marco Longobardo, "Factors Relevant for the Assessment of Sufficient Gravity in the ICC. Proceedings and the Elements of International Crimes", 3 *Questions of International Law* (2016), p. 40, http://www.qil-qdi.org/wp-content/uploads/2016/11/03_ICC-Gravity-Test-_LONGOBARDO_FIN-2.pdf.

[71] See *infra*, Section VI.

[72] Situation in Kenya, Decision on the Confirmation of Charges Pursuant to Article 61(7)(a) and (b) of the Rome Statute, Pre-Trial Chamber II, ICC-01/09-02/11-382-Red, 23 January 2012, para. 46. In the 2016 Policy Paper on Case Selection and Prioritisation, the OTP stated that it "considers that the responsibility of commanders and other superiors under article 28 of the Statute is a key form of liability, as it offers a critical tool to ensure the principle of responsible command and thereby end impunity for crimes and contribute towards their prevention" (Policy Paper on Case Selection and Prioritisation, 15 September 2016, para. 36). It has been observed that "command responsibility is most likely to trigger liability when cyber units are integrated into the army and are part of regular operations" (Elies van Sliedregt, "Command Responsibility and Cyberattacks", 21 *Journal of Conflict and Security Law* (2016), p. 521).

resulted from the abuse of power or official capacity, and elements of particular cruelty, including the vulnerability of the victims, any motives involving discrimination, or the use of rape and sexual violence as a means of destroying groups''.[73] The different degrees of participation that characterize individuals involved in cyber operations have already been mentioned.[74] The means employed to execute the crime, in our case, are malware and cyber infrastructures like computers and servers, which are unlikely to be an aggravating factor as such (unlike, for instance, the use of electrocution, machetes and prohibited weapons).[75] Intent might be difficult to discern in the cyber context, as malware can function unpredictably due to technical errors or insufficient knowledge of the targeted systems. Cyber operations, however, can be characterized by cruelty, for instance in the case of a cyber operation that changes the medical data of patients so that they receive the wrong, painful or unnecessary treatment.

It has been suggested that the context of an aggressive war is also an aggravating factor in the evaluation of gravity.[76] The cyber espionage group Fancy Bear, for instance, has been accused of infecting, under the instructions of Russia, an ''app'' that allowed the Russian forces to access phone communications and localisation data of the Ukrainian artillery and thus to attack it. This was of course not a war crime as the target was a military objective, and it was not even an attack under

[73] OTP, 2013 Policy Paper on Preliminary Examinations, *supra* note 27, para. 64. In the Report on the *Mavi Marmara*, for instance, the Prosecutor looked at whether the alleged crimes were ''systematic or resulted from a deliberate plan or policy to attack, kill or injure civilians or with particular cruelty'' (Situation on Registered Vessels of Comoros, Greece and Cambodia, Article 53(1) Report, *supra* note 21, para. 140).

[74] See *supra*, Section IV.

[75] Cruelty, for instance, was emphasised by the PTC in Situation in Kenya, Decision Pursuant to Article 15 of the Rome Statute, *supra* note 24, paras. 192, 199; and Situation in Burundi, Decision Pursuant to Article 15 of the Rome Statute, *supra* note 27, para. 188.

[76] William A. Schabas and Mohamed M. El Zeidy, ''Article 17'', in Otto Triffterer and Kai Ambos (eds.), *The Statute of the International Criminal Court. A Commentary* (3rd ed., München/Oxford/Baded-Baden: C.H. Beck-Hart-Nomos, 2016), p. 815. See also the Comoros' letter of referral in relation to the *Mavi Marmara*, 14 May 2013, para. 25, https://www.icc-cpi.int/iccdocs/otp/Referral-from-Comoros.pdf.

Article 49(1) of the 1977 Protocol I Additional to the 1949 Geneva Conventions on the Protection of Victims of War.[77] But assuming, for the sake of argument, that it did constitute a war crime, the fact that it was committed in the context of Russia's aggression against Ukraine would be – according to the above opinion – an aggravating factor. This view, however, is not persuasive, for at least two reasons. First, it is unclear how the Prosecutor could establish, at the preliminary examination stage, that the context is that of an aggressive war, i.e. a *jus ad bellum* violation, particularly if the Court cannot exercise its jurisdiction over the crime of aggression in that situation or case. Secondly, considering the context of an aggressive war as an aggravating factor risks conflating the *jus ad bellum* and the *jus in bello* and thus undermining the principle of the equality of belligerents. The ICC has so far not supported the view that the context of an aggressive war is an aggravating factor in the evaluation of gravity.

5.4 *Impact*

Impact can result, among others, from "the sufferings endured by the victims and their increased vulnerability; the terror subsequently instilled, or the social, economic and environmental damage inflicted on the affected communities".[78] Impact, then, has two aspects: the direct impact on the victims and the broader impact on the community.[79] According to the PTC, the impact beyond the victims can be relevant in order to determine sufficient gravity, but its absence does not necessarily negate gravity.[80]

---

[77] On when a cyber operations constitutes an "attack" under the law of armed conflict, see Roscini, *supra* note 10, pp. 178–182. On cyber espionage and the law of armed conflict, see also Marco Longobardo, "(New) Exploitation and (Old) International Humanitarian Law", 77 *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht* (2017), pp. 809–134.

[78] OTP, 2013 Policy Paper on Preliminary Examinations, *supra* note 27, para. 65. See also Situation in the Republic of Kenya, Request for Authorisation of an Investigation pursuant to Article 15, ICC-01/09-3, 26 November 2009, paras. 56, 59.

[79] Stegmiller, *supra* note 30, p. 561. In the *Mavi Marmara* decision, in order to measure the impact beyond the victims the PTC refers to the fact that the events were highly publicised and that several fact-finding missions resulted from the incident (Situation on 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, *supra* note 29, para. 48).

[80] *Ibid.*, para. 47. It has been noted that the impact criterion, like the controversial "social alarm" factor used in the much criticised decision of the PTC in Situation in the DRC, Decision on the Prosecutor's Application for Warrants of Arrest, Article

The inclusion of this factor in the assessment of gravity entails that even cases that result in a low number of victims on the basis of quantitative requirements might be grave enough from a qualitative perspective if they have significant impact.[81] For instance, cyber attacks resulting in death of peacekeepers and humanitarian workers could have a substantial impact because of the importance of peacekeeping and humanitarian missions and of the deterrent effect they could have on them.[82] Cyber attacks committed to influence political elections might also have a significant impact on the community.[83] In August 2017, for instance, the Kenyan opposition claimed that hackers had manipulated the results of the recent elections by breaking into the database of Kenya's electoral commission so to acquire data on the electorate and draft a targeted campaign strategy.[84] This is, as such, not an international crime, but at least 24 people were killed in the violence that erupted after the contested re-election of President Kenyatta.[85] Certain cyber attacks might also have repercussions on a country's economy, as in the case of the 2007 DDoS attacks against Estonia. More in general, cyber attacks that target national critical infrastructures, thus disrupting the provision of essential services to the society, will have more significant impact

---

Footnote 80 continued
58, *supra* note 24, paras. 47, 64, 67, 77 (decision subsequently reversed by the Appeals Chamber, Situation in the DRC, Judgment on the Prosecutor's Appeal against the Decision of Pre-Trial Chamber I, *supra* note 37, para. 72), is more a policy than a legal criterion and should therefore be applied only in relation to relative gravity (Ambos, *supra* note 23, p. 287).

[81] For Heller, however, "[i]t is almost unconceivable that, when committed in isolation, even the most systematic and socially alarming crimes with relatively few victims could create the kind of situation that would draw the OTP's attention" (Heller, *supra* note 69, p. 243).

[82] Situation in Darfur, Sudan, Decision on the Confirmation of Charges, *supra* note 33, para. 33; Situation in Georgia, Decision on the Prosecutor's Request for Authorization of an Investigation, *supra* note 27, para. 55.

[83] Heller, *supra* note 69, pp. 236–237.

[84] Talita De Souza Dias, "Propaganda and Accountability for International Crimes in the Age of Social Media: Revisiting Accomplice Liability in International Criminal Law", Opinio Juris, 4 April 2018, http://opiniojuris.org/2018/04/04/propaganda-and-accountability-for-international-crimes-in-the-age-of-social-media-revisiting-accomplice-liability-in-international-criminal-law.

[85] As has been observed, "the use of social media to manipulate elections and to provide other types of assistance to international crimes can potentially give rise to individual criminal responsibility under international law" (De Souza Dias, *supra* note 84).

on the broader community than those on other infrastructures, especially if their effects are long-term. Not only social and economic damage should be considered in this context, however, but also that to the natural environment: one could think, for instance, of a cyber attack on a chemical plant intended to cause the release of hazardous substances into the ocean during an armed conflict.[86]

VI LEGAL AND RELATIVE GRAVITY OF SITUATIONS AND CASES INVOLVING CRIMINAL CONDUCT IN CYBERSPACE

The Prosecutor has so far not clearly distinguished between legal and relative gravity in the application of the above mentioned factors, i.e. between gravity as an admissibility threshold and gravity as a discretional factor in the selection and prioritisation of cases.[87] It seems, however, that, for *legal* gravity, the threshold should not be very high.[88] Indeed, ''the gravity threshold appears essentially to provide a backstop ensuring that the Court rejects cases of crimes that technically meet the definitions in the Statute, but are nonetheless minor''.[89] As Ambos notes, ''the 'definitional gravity' of the ICC crimes entails a presumption in favour of legal gravity and [...] the additional gravity threshold is practically only relevant with regard to war crimes''.[90] The result is that, in practice, legal gravity should essentially preclude investigation and prosecution only of small scale, isolated war crimes, but generally not of acts of genocide or crimes against humanity, i.e. crimes which are grave per se.[91] Only an isolated cyber attack against protected persons or objects in the context

[86] The 2016 Policy Paper suggests that ''the Office will give particular consideration to prosecuting Rome Statute crimes that are committed by means of, or that result in, *inter alia*, the destruction of the environment, the illegal exploitation of natural resources or the illegal dispossession of land'' (2016 Policy Paper, *supra* note 72, para. 41).

[87] Stegmiller, *supra* note 23, p. 331.

[88] Stegmiller, *supra* note 23, p. 351.

[89] DGuzman, *supra* note 18, p. 1440.

[90] Ambos, *supra* note 23, p. 294.

[91] DeGuzman, *supra* note 18, p. 1457–1458; Stegmiller, *supra* note 23, pp. 351, 355. For Stegmiller, legal gravity can be applied only exceptionally to crimes against humanity and aggression. The PTC has also found that torture is a crime which is grave ''per se'' (Situation in the Islamic Republic of Afghanistan, Decision Pursuant to Article 15 of the Rome Statute, *supra* note 22, para. 85).

of and associated with an armed conflict which results in negligible damage and little impact, therefore, would not cross the legal gravity threshold.[92] On the other hand, cyber conduct constituting, instigating or facilitating an act of genocide will not need to result in a high number of casualties to be considered admissible. The same low threshold should be applied to the assessment of the legal gravity of both situations and cases: ''in the first scenario, the crimes of the overall situation are evaluated; in the second scenario, just the crimes within the specific case can be evaluated''.[93]

It is in the assessment of *relative* gravity for the selection and prioritisation of situations and cases that the Prosecutor has broader discretion.[94] Indeed, ''the relative gravity threshold is rather high, in any case higher than the legal gravity threshold''.[95] This is confirmed in a Policy Paper on Case Selection and Prioritisation published by the OTP in 2016, which states that ''the Office may apply a stricter test when assessing gravity for the purposes of case selection than that which is legally required for the admissibility test under article 17''.[96] As Ambos notes, the individual circumstances of the alleged perpetrator, including their role as ''most responsible'' in the commission of the crime, could be taken into account when assessing the relative, not legal, gravity of a case.[97] Furthermore, quantitative and qualitative criteria can be considered on an equal basis in the relative gravity evaluation.[98] Finally, relative gravity allows for decisions made on a comparative basis between pending and potential cases before the Court.[99] Even cases involving cyber conduct that could be

[92] Stegmiller, *supra* note 23, p. 352.

[93] Stegmiller, *supra* note 23, p. 354.

[94] As Ambos notes, however, the Prosecutor ''must act independently, impartially, and objectively investigating all parties to a conflict without favouring or discriminating against any one of them'' (Ambos, *supra* note 23, p. 378). See also Carsten Stahn, *A Critical Introduction fo International Criminal Law* (Cambridge: Cambridge University Press, 2019), p. 348.

[95] Ambos, *supra* note 23, p. 294.

[96] 2016 Policy Paper, *supra* note 72, p. 13, para. 36.

[97] Ambos, *supra* note 23, p. 293.

[98] Stegmiller, *supra* note 23, p. 352. For Ambos, qualitative factors should be applied primarily to relative gravity and only exceptionally to gravity as an admissibility threshold, while quantitative factors can be applied in both contexts (Ambos, *supra* note 23, pp. 293, 295).

[99] Stegmiller, *supra* note 23, p. 355. Comparative gravity analysis in the context of admissibility, on the other hand, is problematic (Stahn, *supra* note 94, p. 330).

considered admissible under Article 17, therefore, might not be investigated or prosecuted by the OTP if the number of victims is significantly lower than in other comparable cases. On the other hand, it is not to be excluded that the Prosecutor might decide to select certain situations and cases involving the commission, instigation or facilitation of international crimes through cyber conduct because of their impact or to deter them in the future, even if they resulted in a lower number of victims than in other cases.[100]

VII CONCLUSIONS

It is entirely possible that certain situations and cases involving cyber conduct that constitutes, instigates or facilitates international crimes under the ICC jurisdiction could be considered admissible from a gravity perspective. As has been seen, cyber conduct can potentially satisfy all the factors identified by the Court for the determination of gravity. As with crimes committed by traditional means, legal gravity, as an admissibility threshold, should not be a bar to the investigation or prosecution of acts of genocide and crimes against humanity committed, instigated or facilitated through cyber means, and should only be applied to cyber war crimes in order to exclude "those committed in isolation from other crimes, causing the least harm, and by the lowest level perpetrators".[101]

Whether the Prosecutor will actually decide to select and prioritise admissible situations and cases involving cyber conduct over other situations and cases is a matter that falls within her prosecutorial discretion, and in which quantitative and qualitative gravity factors can be taken into account on an equal basis together with the subjective circumstances of the alleged perpetrator and pragmatic and operational considerations: the Prosecutor, then, might decide to investigate or prosecute one case involving cyber conduct but come to

[100] The 2016 Policy Paper states that the OTP "will pay particular attention to crimes that have been traditionally under-prosecuted" in order to help end impunity and prevent such crimes (2016 Policy Paper, *supra* note 72, p. 15, para. 46). On the problems raised by "thematic" investigation and prosecution, see Stahn, *supra* note 94, pp. 350–351.

[101] DeGuzman, *supra* note 18, p. 1458.

a different conclusion in another because of comparative considerations, the likelihood of identifying and apprehending the suspect, or the availability of evidence.[102]

OPEN ACCESS

[102] 2016 Policy Paper, *supra* note 72, pp. 16–17.