7

Contributing to Cyber Peace by Maximizing the Potential for Deterrence

Criminalization of Cyberattacks under the International Criminal Court's Rome Statute

Jennifer Trahan[*]

1 INTRODUCTION

This chapter examines how a cyberattack (i.e., a cyber-enabled malicious activity) that has consequences similar to a kinetic or physical attack (causing serious loss of life or physical damage) could be encompassed within the crimes that may be prosecuted before the International Criminal Court (ICC). The chapter overviews when and how such a cyberattack could fall within the ambit of the ICC's crimes – genocide, crimes against humanity, war crimes, and the crime of aggression. The chapter additionally acknowledges some of the limitations as to which attacks would be encompassed, given, particularly, the gravity threshold of the ICC's Rome Statute, as well as the hurdle of proving attribution by admissible evidence that meets the standard of proof beyond a reasonable doubt. Notwithstanding such limitations, there is still potential for use of the Rome Statute to encompass a limited subset of cyberattacks. Increased awareness of this previous largely overlooked potential could possibly contribute to deterring such crimes, as could prosecution of those cases of cyberattacks that meet the standard of proof by required by the ICC Rome Statute. While it is very difficult to measure the deterrent impact of tribunals and international criminal law, whatever possible deterrence that can be created is certainly

[*] Clinical Professor, NYU Center for Global Affairs and Director of the Concentration in International Law & Human Rights. A more extensive version of the topics addressed herein will appear in Jennifer Trahan, "Criminalization of Cyber-Attacks under the International Criminal Court's Rome Statute" (Trahan, forthcoming). The author thanks Pano Yannakogeorgos for aiding her understanding of cyber operations. She also greatly benefitted from discussions at meetings of the Council of Advisers on the Application of the Rome Statute to Cyberwarfare. The author additionally benefitted from workshopping her chapter at the April 17 and September 25, 2020 workshops hosted by the Ostrom Workshop Program on Cybersecurity and Internet Governance at Indiana University, and particularly appreciates the comments of her discussant, Asaf Lubin. She also benefitted from workshopping the chapter at the June 29–30, 2020 International Criminal Court Scholars' Forum, and particularly appreciates the comments of her discussant, Elies van Sliedregt, and those of Matthew E. Cross, Erin Lovall, Kara McDonald, and Samantha Wynne who provided research assistance.

worth maximizing. This chapter explores how international criminal law could potentially contribute to the goal of reaching a state of "cyber peace." Admittedly, the Rome Statute would not encompass the vast number of cybercrimes that occur, as it would only cover the more severe cyberattacks, such as those inflicting serious loss of life or significant physical damage; however, the Rome Statute *does* have applicability in this area to cover at least a limited subset of cyber operations, and this potential should be explored and utilized. The ICC can only help contribute to deterrence and cyber peace if the ability of the ICC to prosecute certain cyberattacks becomes acknowledged and well known.

2 BACKGROUND

Cyberattacks can take a variety of forms including those aimed at data theft (stealing corporate information) (Griffiths, 2015; as cited in Jensen, 2017, p. 736, n. 6), extortion, the spreading of false information (Greenfield, 2013; as cited in Jensen, 2017, p. 736, n. 7), manipulation of elections (Hathaway et al., 2012, p. 819; Ohlin, 2020), breach of government computers in an effort to steal state secrets (O'Hare, 2016; as cited in Jensen, 2017, p. 737, n. 8,), as well as denial of service attacks (U.S. Department of Homeland Security and the Cybersecurity and Infrastructure Security Agency [CISA], 2019). Such attacks sometimes proliferate beyond their intended targets to impact information technology (IT) systems around the globe, as with the infamous NotPetya attack (Greenberg, 2018; Efrony & Shany, 2018, pp. 628–631). Further, the software code used in cyberattacks may also be "repurposed" by others (Bellovin et al., 2017). Fortunately, to date, cyberattacks and cybercrimes have not resulted in widespread devastation causing loss of life and, to the extent physical damage has resulted, such damage has occurred more to data, computer hardware and software and, in one instance, to centrifuges at a nuclear facility (the Stuxnet attack). Cyberattacks have also caused massive economic losses (Greenberg, 2018) and compromised the personal information of millions of individuals (Jensen, 2017, p. 737).

The use of cyber technology to date, however, makes clear that a much more catastrophic cyberattack could occur. States (on their own, or in conjunction with nonstate actor/hacker groups) now have the capacity to combine cyber weapons with conventional weapons into a "blended attack," such as occurred in Ukraine (Greenberg, 2018) and Georgia (ICC Forum, 2018). A number of war crimes that could be committed during a conventional armed conflict could now, potentially, also be committed through the use of cyberattacks or through both cyber and conventional means. Absent a state of armed conflict, cyberattacks meeting the requirements of, *inter alia*, a widespread or systematic attack against a civilian population could fall within the ambit of "crimes against humanity." For example, the technological capacity to disable air traffic controls exists, causing a "cyber 9/11" – perpetrated, for example, by nonstate actors (cyber criminals or bands of hackers). A cyberattack could similarly target computer systems that control train traffic, nuclear

facilities (Greenberg, 2017a), hospitals (Glaser, 2017; Mačák et al., 2020), power grids (Greenberg, 2017b, 2018), and other critical infrastructure – or, for example, a dam located upstream from a major city (Berger, 2016). It is this narrow subset of cyberattacks – causing serious loss of life and/or physical destruction – *not* the vast number of cybercrimes being perpetrated – that this chapter addresses.

While one hopes that a large-scale cyberattack, or even a more limited one that causes serious loss of life or damage to physical objects, will never reach fruition, it is simultaneously helpful to acknowledge that should such an attack occur, it potentially could be covered by one or more of the crimes provided for under the ICC's Rome Statute. States, particularly Rome Statute States Parties, could also incorporate Rome Statute crimes into their domestic criminal codes and statutory law (if they have not already done so), and/or develop additional laws criminalizing cyberattacks and/or cybercrimes. Should they do so, domestic definitions of the crimes could be more broadly formulated than their Rome Statute counterparts and have greater jurisdictional reach; thus, the limitations of the Rome Statute discussed in this chapter do not necessarily carry over to domestic jurisdictions. While the international community could also create a new international criminal tribunal to deal exclusively with cybercrime and cyberattacks, in light of the apparently unwillingness to create new criminal tribunals[1] this chapter focuses on the permanent international criminal tribunal that already exists, the ICC.

3 MAXIMIZING THE POTENTIAL FOR CYBER PEACE THROUGH DETERRENCE

The goal of the present chapter is not only to make the case for ICC cyber prosecutions should a horrific attack occur but to increase awareness of the potential for ICC prosecutions in order to maximize the potential for deterrence as a means to contribute to achieving a state of "cyber peace" (see Shackelford, 2017, p. 8, defining "cyber peace"). It is important that the cyber domain is not seen as unfettered by the rule of law, when it is in fact subject to numerous bodies of international law (UK Government, 2018; Koh, 2012, p. 3), including international humanitarian law (aka the laws of war) (Schmitt, 2017, Rule 80; "The Paris Call," 2018), international human rights law (Schmitt, 2017, Rule 35), as well as the use of force norms contained within the UN Charter as supplemented by customary international law (Schmitt, 2019 (citing position of France, and the UK Government, 2018, noting also that Russia and China accept that the UN Charter applies in cyberspace)). The more well acknowledged it is that international humanitarian law and international human rights law apply in the cyber domain, the easier it is to make the case

[1] Recently, for example, the international community has created three investigative mechanisms – to investigate crimes committed in Syria, Myanmar, and Iraq (if perpetrated by the so called "Islamic State" (ISIL) – but has not created tribunals for the prosecution of those crimes (see Trahan, 2021).

https://doi.org/10.1017/9781108954341.007 Published online by Cambridge University Press

that certain cyberattacks are covered under international criminal law. Even if the application of current bodies of international law to cyberattacks may not prove an "elegant fit," it is imperative to utilize the laws that exist and/or develop additional laws (cf. Rona, 2003, p. 60, arguing International Humanitarian Law (IHL) should apply to the "war on terror" even if "not an elegant fit").

Significant academic literature exists on the subject of whether international criminal law can play a deterrent role and whether the existence of the various *ad hoc* and hybrid criminal tribunals has contributed to deterrence and/or the ICC can do so.[2] Various scholars take a pessimistic stance as to the potential of tribunals to deter atrocity crimes (McAllister, 2019–20, p. 85, n. 2, categorizing scholars as "deterrence pessimists"). Yet, increasingly, there are scholars whose studies yield positive results (McAllister, 2019–20, p. 85, n. 4, categorizing scholars as "deterrence optimists"). For example, a recent study, based on over 200 interviews, demonstrates that Macedonian Armed Forces, during the 2001 conflict in Macedonia, considered the existence of the International Criminal Tribunal for the former Yugoslavia (ICTY) when deciding their actions (specifically, whether any could be viewed as war crimes), and this deterred violence against civilians (McAllister, 2019–20; see also Schense & Carter, 2017). Similar studies show some deterrence created by the existence of the ICC (Jo & Simmons, 2016; Hillebrecht, 2016; Human Rights Watch, 2009, Ch. IX).

It is worth noting that domestic criminal law also does not fully deter domestic crimes; yet states nonetheless criminalize crimes, from murder to insider trading. So too with international criminal law. As Brierly observes: "States often violate international law, just as individuals often violate municipal law" (Brierly, 1944, pp. 4–5). Clearly, the field of international justice has not yet fully deterred crimes such as genocide, crimes against humanity, or war crimes, as these crimes still occur far too often. Furthermore, it is also notoriously hard to prove a negative – that is, that crimes have *not* occurred due to the deterrent impact of tribunals or international criminal law – so there could actually be more deterrence than can be conclusively demonstrated. Yet, the case that one should *not* criminalize atrocity crimes is generally not made; clearly, whatever role deterrence can play is worth maximizing, and if international criminal laws and tribunals are incapable of deterring or not fully capable of doing so, then at least the laws exist whereby the crimes may be prosecuted. In short, international criminal law is one of the tools at the disposal of those working in the field of international justice, and while it may not fully deter, any deterrence potential is useful. As Guido Acquaviva writes: "international criminal institutions" that "strengthen[] the rule of law and pursu[e] individual criminal

[2] The *ad hoc* tribunals refer to the International Criminal Tribunal for the former Yugoslavia (ICTY) and the International Criminal Tribunal for Rwanda (ICTR). The "hybrid tribunals" include the Special Court for Sierra Leone, the Extraordinary Chambers in the Courts of Cambodia, the hybrid War Crimes Chamber of the Court of Bosnia and Herzegovina in Sarajevo (State Court), the Special Tribunal for Lebanon, and the Kosovo Specialist Chambers.

responsibility" "can increase awareness of the primary rules … among the general public and … foster compliance with the law and therefore, indirectly, general deterrence" (Acquaviva, 2014, p. 786).

The United States, for instance, suggests that the prosecution of cyberattacks *can* change behavior. Kristen Eichensehr explains:

> One of the most often-cited purposes of public attributions [of cyberattacks] is macro-level deterrence. The idea is that public naming-and-shaming of state-sponsored actors will cause the named states (and potentially other states that might be watching) to refrain from future attacks. For example, in announcing an indictment of Iranian hackers for [Distributed Denial of Service ("DDOS")] attacks on U.S. financial institutions, then-FBI Director James Comey explained, "By calling out the individuals and nations who use cyber attacks to threaten American enterprise, as we have done in this indictment, we will change behavior." U.S. officials made similar claims about the cyber sanctions executive order. In announcing the new sanctions regime, the Obama Administration's Cybersecurity Coordinator, Michael Daniel called it "a new way of both deterring and imposing costs on malicious cyber actors wherever they may be." (Eichensehr, 2020, p. 552)

Eichensehr notes that: "After the first U.S. attribution-by-indictment – the charges against Chinese [People's Liberation Army] officers for intellectual property theft – sources indicated that the Chinese military substantially scaled down its economic espionage activities. But at the same time, [Eichensehr admits] state-sponsored hacks of many kinds have continued after indictments" (Eichensehr, 2020, p. 553). Eichensehr also discusses what she calls "micro-level deterrence" against particular individuals who are deterred from future violations through indictment or the imposition of sanctions (Eichensehr, 2020, pp. 554–555). Certainly, the potential for deterrence is maximized through the use of international criminal law, which has the potential to contain far more stringent sanctions than simply "naming and shaming" – that is, simply publicly attributing the source of the cyberattack.

That said, as mentioned, the ICC cannot play a role in deterring cyberattacks unless actors (both state and nonstate actors) *realize* that certain cyberattacks, even if only a limited subset of them, *could* constitute Rome Statute (or other) crimes. In this respect, one welcome initiative is the convening of the "Council of Advisers on the Application of the Rome Statute to Cyberwarfare," a group of expert participants convened by the Permanent Mission of Liechtenstein to the United Nations and co-organized by Argentina, Austria, Belgium, Costa Rica, the Czech Republic, Estonia, Luxembourg, Portugal, Spain, and Switzerland, as well as the Global Institute for the Prevention of Aggression ("Council of Advisers," 2021). The goal of the group is to increase awareness of the potential for the Rome Statute to cover certain cyberattacks through its meetings and the eventual release of a report (see also Digital Watch discussing the Open Ended Working Group on Cybersecurity at the UN). (The author serves on the Council of Advisers.)

It is not claimed that this increased knowledge will fully deter cyberattacks that could be encompassed by the Rome Statute; in particular, one would expect less deterrence in situations where no ICC jurisdiction exists, and where one would not anticipate the Security Council referring a situation to the ICC (see the Rome Statute, 1998, Arts. 12(2)(a)–(b), 13(b), 15*bis*, 15*ter* on jurisdiction).[3] For example, it would be naïve to anticipate referral by the Security Council of a situation to the ICC (which is permitted, Rome Statute, 1998, Arts. 13(b), 15*ter*), if a permanent member of the Security Council is involved in a cyberattack. (The permanent members hold veto power over substantive Security Council votes, UN Charter, Art. 27(3)). Additionally, it might be difficult to deter informal or rogue bands of hackers who might remain unaware of any expert report on cyberattacks (or even the ICC's existence), and perhaps would not be deterred regardless. An additional argument could be made that the ICC would have to become a more effective institution before it creates significant deterrence – for example, it has a significant number of outstanding arrest warrants (see ICC Warrant/Summonses, n.d.). Furthermore, that the ICC tends to focus its prosecutions on higher-level perpetrators further suggests that "ordinary hackers" would not necessarily fall within its focus absent an egregious cyberattack, and so decreases any deterrence potential to "ordinary hackers." Yet, the ICC is not limited to prosecuting only those bearing the "greatest responsibility" for statutory crimes, as was, for example, the Special Court for Sierra Leone (Special Court Statute, Art. 1.1); thus, if a particularly egregious cyberattack were to occur, an "ordinary hacker" could potentially attract the ICC Prosecutor's focus, including, potentially, all who aided and abetted the crime or who acted with the "common purpose" of committing the crime.[4] Notwithstanding, as mentioned, the initial first step in attempting to maximize deterrence – and thereby potentially contributing to the goal of achieving a state of cyber peace – is most certainly to create broader awareness of the ICC's potential to prosecute a limited subset of cyberattacks.[5]

The section below briefly considers two initial overarching considerations that restrict the cyberattacks the ICC might be able to prosecute. The following

[3] As to the crimes of genocide, war crimes, and crimes against humanity, the ICC has jurisdiction over crimes committed: (1) in the territory of Rome Statute States Parties; (2) by the nationals of Rome Statute States Parties, or; (3) within situations referred by the Security Council (Rome Statute, 1998, Arts. 12(2)(a)–(b); 13(b)). A state may also accept jurisdiction by entering a declaration pursuant to Article 12(3). There is a different and more restrictive jurisdictional regime for the crime of aggression, including that there is *no* jurisdiction over crimes committed in the territory of, or by the nationals of, non-States Parties (Rome Statute, 1998 Art. 15*bis*, para. 5). Referrals by the Security Council are also permitted covering the crime of aggression (Rome Statute, 1998, Art. 15*ter*).

[4] For background on individual criminal responsibility, including "aiding and abetting" and the "common purpose" doctrine, see Ambos, 2016b.

[5] For another analysis of how cyberattacks could fall within the ICC's definitions of war crimes and crimes against humanity, but finding it difficult to envision them constituting the crime of aggression, see Ambos, 2015.

section provides a brief overview of how certain cyberattacks could fall within the Rome Statute's substantive crimes – war crimes, crimes against humanity, genocide, and the crime of aggression. A more expansive discussion of both topics can be found in my forthcoming article "The Criminalization of Cyberattacks under the International Criminal Court's Rome Statute" (Trahan, forthcoming) and the upcoming Report of the Council of Advisers on the Application of the Rome Statute to Cyber Warfare (forthcoming).

4 OVERARCHING CONSIDERATIONS AS TO ICC PROSECUTIONS

Some of the limiting factors in terms of prosecuting cyberattacks before the ICC include (1) the Rome Statute's "gravity" threshold and (2) the need to prove attribution through admissible evidence that could satisfy the standard of proof beyond a reasonable doubt. While they are beyond the scope of the present chapter, additional limiting factors include the need to satisfy jurisdiction; the ICC's "intent" requirement (which excludes responsibility for unforeseen consequences and severely restricts it even as to foreseeable consequences);[6] and the prohibition in the Rome Statute on expanding definitions of crimes by analogy, with ambiguity construed to favor the defense (Rome Statute, 1998, Art. 22(2)). (For a discussion of all three topics, see Trahan, forthcoming.)

5 THE ICC'S GRAVITY THRESHOLD

For a case to be "admissible" before the ICC, Article 17 of the Rome Statute requires that it be of "sufficiently gravity to justify … action by the Court" (Rome Statute, 1998, Art. 17(1)(d)). Article 53 further states that the Prosecutor may only initiate an investigation or proceed with a case if it "would be admissible under Article 17" (Rome Statute, 1998, Arts. 53(1)(b), 53(2)(b)). These provisions raise the question of which cyberattacks would be considered more grave and which less grave, or of marginal gravity. The ICC's cases to date have focused on rather large-scale crime scenes, with the "smaller" crime scenes probably being the killing of twelve peacekeepers, at issue in the *Abu Garda* case (see Whiting, 2015),[7] and the destruction of nine mausoleums and one mosque at issue in the *Al Mahdi* case (*Prosecutor* v. *Al Mahdi*, Case Information

[6] "The *Lubanga* appeal judgment confirmed the interpretation put forward in the *Bemba* decision on the confirmation of charges, that under Art. 30 … 'the standard for the foreseeability of events is virtual certainty.'" (Badar & Porro, 2017, Art. 30(2)(b), *citing Prosecutor* v. *Lubanga*, 2014, ICC A. Ch., "Judgment on the Appeal of Mr. Thomas Lubanga Dyilo against his conviction," paras. 441 *et seq.*; *Prosecutor* v. *Bemba*, 2009, ICC PT. Ch., "Decision Pursuant to Article 61(7)(a) and (b)," paras. 359 *et seq.*) If the ICC remains consistent with this approach, it would mean that criminal responsibility for unforeseeable consequences would be excluded and even for foreseeable consequences, the standard would be "virtual certainty" that the consequences will result.

[7] The author in no way means to minimize the severity of these crimes.

https://doi.org/10.1017/9781108954341.007 Published online by Cambridge University Press

Sheet, 2018). Both cases involved the killing of persons or the destruction of physical objects.[8]

In terms of evaluating the gravity of cyberattacks, a useful starting point for analysis is *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Tallinn 2.0). Admittedly, there are divergent views among states and experts as to the weight to accord the Tallinn Manual (Efrony & Shany, 2018), and in any event they are not binding on the ICC, yet they can at least provide a useful starting point.

In Tallinn 2.0, the experts focused on what constitutes an "armed attack" committed through cyber means. They engaged in this analysis because an "armed attack" can justify self-defense under Article 51 of the UN Charter (see UN Charter, Art. 51); they were not engaging in this analysis in relationship to the ICC. Tallinn 2.0 takes the position that "a cyber operation that seriously injures or kills a number of persons or that causes significant damage to, or destruction of, property would satisfy the scale and effects requirement" and thus constitute an "armed attack" (Schmitt, 2017, Rule 71, para. 8.) This would provide one possible standard by which to evaluate the gravity of cyberattacks. Namely, only if a cyberattack seriously injures or kills a number of persons or causes significant damage to, or destruction of, property, would that satisfy Rome Statute gravity.

The experts additionally suggested various criteria that "States are likely to consider" as to when a cyber operation constitutes a "use of force" (relevant to considering when Article 2(4) of the UN Charter is violated, see UN Charter, Art. 2(4)). These criteria included severity, immediacy, directness, invasiveness, and measurability of effects (Schmitt, 2017, Rule 69, para. 9 (a)–(e)). These would appear useful criteria to consider in making the gravity evaluation. Additional factors that could prove useful for consideration include those identified in ICC case law (see, e.g., *Prosecutor* v. *Al Hassan*, 2020, paras. 59, 89, 90) and by the Prosecutor (see "Policy Paper on Preliminary Examinations," 2013, paras. 62, 64–65).

Another interesting consideration is whether loss of life or physical destruction is always the most grave of harms? For instance, France takes the position that operations that penetrate military systems to weaken French defensive capabilities, even if this does not produce physical effects, would constitute a "use of force" (Droit International, 2019, as cited in Schmitt, 2019).[9] Similarly, the Netherlands takes the view that a catastrophic systems attack that causes very serious economic impact could constitute an "armed attack" (Schmitt, 2019, quoting the Dutch Minister of Defence). While neither country is opining on whether such conduct would meet Rome Statute gravity, it is worth considering whether it should do so. The author suggests that here one might differentiate between penetration of military systems and catastrophic systems attacks that cause serious

[8] For a general discussion of gravity, see deGuzman, 2020. See also n. 10 (discussing the OTP's not proceeding in the *Comoros* case where there were ten fatalities).

[9] For France's most significant statement regarding the application of international law in cyberspace, see Droit International, 2019, as cited in Schmitt, 2019.

injuries or fatalities to persons, or significant damage to or destruction of property, from those that do not. Another interesting question is whether the destruction of "data" should be encompassed, or whether the "property" destroyed would need to be physical property (see, e.g., Biller and Schmitt, 2019; Mačák, 2015; Horowitz, 2020, considering destruction of data).

The ICC might wish to examine these issues and consider issuing a policy paper on application of the Rome Statute to cyberattacks (including the topic of gravity). At the same time, in terms of increasing deterrence potential, there could also be some advantages flowing from ambiguity. Thus, this author suggests that one possible gravity threshold for ICC prosecution could be where a cyberattack causes serious injuries or fatalities to persons or significant damage to or destruction of property; at the same time, perhaps one would not want to close the door to other large-scale or invasive attacks that do not meet this definition. Also, as the ICC Appeals Chamber explains in the *Al Hassan* case, the gravity requirement does not "oblige the Court to choose only the most serious cases, but merely [obliges] it not to prosecute cases of marginal gravity" (*Prosecutor* v. *Al Hassan*, 2020, para. 59).

The ICC's pursuing of a case where a cyberattack of sufficient gravity occurs would be significant in itself, and make clear that the Rome Statute *does* encompass cyberattacks. Roscini writes: "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" (Roscini, 2019, p. 271).[10] This "expressivist" approach – pursuing prosecutions that further protected values and thereby sending a message to achieve a given result – is indeed an important and legitimate aspect of prosecutorial strategy (Cross, 2020, pp. 67–68).

6 Proving Attribution through Admissible Evidence that Establishes Proof Beyond a Reasonable Doubt

An additional limiting factor – true for all ICC crimes – would be that all the elements of the crime would need to be proven through admissible evidence that could eventually satisfy the requirement at trial of proof beyond a reasonable doubt (Rome Statute, 1998, Art. 66(3)). This includes the issue of attribution (who conducted the cyberattack), sourcing it not just to a state (or nonstate actor/hacker group working for the state) but potentially to a particular "computer, … to identify the person who operated the computer, and more importantly to identify the real 'mastermind'

[10] In the *Comoros* case, the ICC's Office of the Prosecutor (OTP) took the position that ten fatalities did not meet the gravity threshold, although there were other considerations than simply the number of fatalities (OTP, Report on Preliminary Examination Activities, 2017, para. 336). In the *Abu Garda* case, as mentioned, the OTP did proceed regarding the killing of twelve peacekeepers "because of the significance of the target and impact on peacekeeping operations" (Whiting, 2015).

behind the attack ….” (Tsagourias, 2012, p. 233). This could pose significant challenges (Dederer & Singer, 2019, p. 438 (citing sources)).

Compounding difficulties, cyberattackers sometimes go to lengths to conceal cyber operations (Hathaway et al., 2012, p. 843), and states sometimes deliberately hide their attack as perpetrated by another state (“false-flagging”). For example, this happened when “Russian hackers piggy-backed on an Iranian cyber-espionage operation,” thereby hacking into “government and industry organizations in dozens of countries while masquerading as attackers from the Islamic Republic [of Iran]” (Stubbs & Bing, 2019). Or states can hide behind nonstate actors to mask their operations (Dederer & Singer, 2019, p. 438; Hathaway et al., 2012, p. 854). Even when that is not the case, because cyberattacks can be perpetrated through a single computer or network of computers located far from where the consequences impact, they can be extremely difficult to attribute (Dederer & Singer, 2019, p. 431; Brenner, 2011, p. 32). The attacks can also be concealed by feigning that operating systems are functioning normally (Rowe, 2007; Hathaway et al., 2012, p. 828).

Furthermore, if attribution is to be made, this raises questions as to who would be in a position to do so. Would this be practical for the ICC to do itself? And, if not, what are the implications of relying on state cooperation in this regard? In addition to attribution, all of the evidence in the case would require “authentication,” and this (and simply having the knowledge to assemble a cyberattack case) would require significant technical expertise. Relying on state cooperation also carries pitfalls in that states may be more likely to cooperate when it suits their self-interests (e.g., they have suffered from a cyberattack), and not cooperate when it does not serve their interests (e.g., they were the perpetrator or linked to the perpetrator). Thus, there will be significant challenges in terms of attribution, authentication, and development of the necessary expertise to establish both. Building ICC expertise will require both the hiring of staff, and/or use of outside experts, and development of relevant policies.

Thus, the above discussion suggests the potential applicability of the Rome Statute to a limited subset of cyberattacks: (1) if they meet the Rome Statute’s gravity threshold and (2) where attribution could be proven beyond a reasonable doubt. As mentioned, other limiting factors include whether jurisdiction exists; whether the “intent requirement” can be proven (which appears to exclude responsibility for unforeseen consequences and limit responsibility even for foreseen consequences);[11] and whether the crimes can be applied without drawing on analogies, with ambiguity construed to favor the defense (Trahan, forthcoming).

7 THE ROME STATUTE’S SUBSTANTIVE CRIMES

Despite the limitations suggested above, the next section outlines the key elements of the Rome Statute’s four core crimes – genocide, war crimes, crimes

[11] See supra note 7.

https://doi.org/10.1017/9781108954341.007 Published online by Cambridge University Press

against humanity, and the crime of aggression – and suggests how a limited subset of cyberattacks might fall within the definitions of each.[12] Again, domestic jurisdictions, even ones that incorporate these crimes into their domestic criminal codes, could adopt broader definitions of the crimes; thus, the elements of the crimes discussed below would not necessarily apply in domestic jurisdictions, which also might have or develop broader criminal statutes covering cyberattacks and/or cybercrimes.

8 CYBERATTACKS AS WAR CRIMES UNDER THE ROME STATUTE

As mentioned, the rules of international humanitarian law apply in the cyber domain (Schmitt, 2017, Rule 80; "The Paris Call," 2018). Thus, for example, Tallinn 2.0 explains that in a state of armed conflict, cyberattacks may not target civilians (Schmitt, 2017, Rule 80), may not be indiscriminate (Schmitt, 2017, Rule 105), and may not cause excessive "collateral damage" (Schmitt, 2017, Rule 113). Tallinn 2.0 expressly acknowledges that when such IHL rules are violated, "[c]yber operations may amount to war crimes and thus give rise to individual criminal responsibility under international law" (Schmitt, 2017, Rule 84).

Under the Rome Statute, "[the] Court shall have jurisdiction in respect of war crimes in particular when committed as a part of a plan or policy or as part of a large-scale commission of such crimes" (Rome Statute, 1998, Art. 8(1)). Additionally, all of the contextual elements for war crimes would need to be proven – such as the existence of an "armed conflict" (whether international or noninternational), a "nexus" between the cyberattack and the armed conflict (ICC, "Elements of Crimes," 2011), and that the perpetrator was aware of the factual circumstances that established the existence of the armed conflict (ICC, "Elements of Crimes," 2011). There would also be the elements for the specific underlying war crime(s), as well as – as explained above – the need to prove attribution (linking a specific perpetrator), intent, and jurisdiction. As to specific war crimes, note that the Rome Statute contains different lists of war crimes depending on whether the crimes were committed during international armed conflict or noninternational armed conflict (*compare* Rome Statute, 1998, Art. 8.2(a)–(b) *with* Art. 8.2(c), (e)).

As to the requirement of armed conflict, under the generally accepted definition from the ICTY's *Tadić* case, "an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State" (*Prosecutor* v. *Tadić*, 1995, para. 70). The Rome Statute (and IHL) particularly

[12] The implications of the author's argument – that certain cyberattacks fall within the Rome Statute's existing crimes – suggests that in terms of retroactivity, jurisdiction for qualifying cyberattacks would be the same as it is for the crimes generally. That is, for initial ratifying States Parties, it could go back to July 1, 2002, and for the crime of aggression it could go back to July 17, 2018.

exclude "situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence or other acts of a similar nature" (Rome Statute, 1998, Art. 8(2)(d)). An international armed conflict is one in which two or more states are parties to the conflict (Rona, 2003, p. 58; Common Article 2 to the 1949 Geneva Conventions). Noninternational armed conflict is defined as "armed conflict not of an international character" (Common Article 3 to the 1949 Geneva Conventions). For noninternational armed conflict, the operations must also have reached a minimum level of intensity and a nonstate armed group must have achieved a certain level of organization (*Prosecutor* v. *Tadić*, 1995, para. 70).[13]

The cyberattacks on Eastern Ukraine provide a possible example of war crimes perpetrated using, at least partly, cyberattacks. The attacks there were "blended attacks," perpetrated through cyber and physical/kinetic means. In addition to the armed conflict that killed more than 10,000, the hacking into dozens of governmental organizations and companies through a "scorched-earth" cyberattack, which penetrated victims ranging from media outlets to railway firms and hospitals, caused hundreds of thousands of homes to lose electricity and shut down at least three regional utilities (Greenberg, 2018; Bezhan, 2016; Efrony & Shany, 2018, pp. 624–626). Both the United States and the United Kingdom believe that the cyberattacks on Ukraine were perpetrated by Russia's military intelligence service, commonly known by the Russian acronym GRU (Warrell et al., 2020).

The cyberattack, conducted during a state of armed conflict could, if all the elements of the crimes were able to be proved through admissible evidence, potentially constitute the war crime of intentionally directing attacks against the civilian population (Rome Statute, 1998, Art. 8(2)(b)(i)), or civilian objects (Rome Statute, 1998, Art. 8(2)(b)(ii)),[14] or inflicting "collateral damage" – incidental loss of life or injury to civilians that is "clearly excessive in relationship to the concrete and direct overall military advantage anticipated" (Rome Statute, 1998, Art. 8(2)(b)(iv)).[15] The cyber operations also appear to have been "indiscriminate."[16] A cyberattack against a medical facility – of which there were several in Eastern Ukraine (Greenberg, 2018) – could also constitute a war crime under Rome Statute Articles 8(2)(b) (xxiv) and

[13] For one analysis of when a cyberattack reaches the threshold of armed conflict, see Ambos, 2015, at pp. 121–126. Ambos also notes that groups of "hackers" may not meet the organization requirement (Ambos, 2015, at pp. 125, 129).

[14] Application of the principle of distinction may, however, be complicated by "the *interconnectivity* between military and civilian computer systems and the mostly *dual-use* of cyber ingrastructure," although "dual-use objects are qualified as military objectives since they normally contribute to military purposes …." (Ambos, 2015, at p. 131) (italics in original).

[15] For analysis of when a civilian "directly participates" in hostilities in the cyber context, so as to become a permissible target, see Ambos, 2016a, at p. 128.

[16] Here, the Rome Statute has a problem. Rome Statute Article 8(2)(b)(xx) prohibits employing weapons that are "inherently indiscriminate," but only for weapons "included in an annex to th[e] Statute"; puzzlingly, there is no such annex (see Clark, 2009). Thus, at present, use of inherently indiscriminate weapons cannot be prosecuted at the ICC (unless their use also happens to constitute another war crime).

(e)(ii) (Mačák et al., 2020). As with all ICC crimes, one would, among other things, additionally need to attribute responsibility to particular individuals for an ICC case to proceed and satisfy the intent requirement, both of which could prove difficult. There is ICC jurisdiction over the events in Ukraine because Ukraine executed an Article 12(3) declaration, accepting the ICC's jurisdiction over crimes committed on its territory from November 21, 2013 to February 22, 2014, and then executed another such declaration covering crimes committed from February 22, 2014 and continuing on an open ended basis. (ICC Investigation, Ukraine, n.d.). Thus, there currently is ICC jurisdiction over cyberattacks that have been and are being committed in Ukraine, as well as jurisdiction over war crimes, crimes against humanity, and genocide more generally.

9 CYBERATTACKS AS CRIMES AGAINST HUMANITY UNDER THE ROME STATUTE

Crimes against humanity are defined in the Rome Statute as acts "committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack" (Rome Statute, 1998, Art. 7(1)). The "attack" against the civilian population is defined as "a course of conduct involving the multiple commission of acts [enumerated in Article 7(1)] against any civilian population, pursuant to or in furtherance of a State or organizational policy to commit such attack" (Rome Statute, 1998, Art. 7(2)(a)).[17] For crimes against humanity, the attack is directed against a civilian population and need not be a military attack or linked to armed conflict (see, e.g., *Prosecutor* v. *Ntaganda*, 2019, para. 662). There are also requirements that the perpetrator's "conduct was committed as part of a widespread or systematic attack directed against a civilian population" (the "nexus" requirement) and that "[t]he perpetrator knew that the conduct was part of or intended the conduct to be part of a widespread or systematic attack directed against a civilian population" (ICC, "Elements of Crimes," 2011). The "underlying crimes" that support a charge (or multiple charges) of crimes against humanity are murder, extermination, enslavement, deportation, imprisonment, torture, rape or sexual violence, persecution, enforced disappearances, apartheid, and other inhumane acts (see Rome Statute, 1998, Art. 7(1)(a)–(k) for details).

Let us assume a "cyber-9/11" scenario, where the attackers have used cyber means to jam the controls of several airplanes, causing them to crash into buildings with ensuing large-scale loss of life. That would likely constitute the crime against humanity of murder if evidence proves that the attack was "widespread" (e.g., impacting a large number of victims) or "systematic" (a coordinated, organized attack) and orchestrated through a "State or organizational policy" (proof of which may be inferred,

[17] See Ambos, 2015, at p. 142 ("While a loosely organized group of hackers acting autonomously would not meet the organization requirement, organized armed groups within the meaning of IHL that take recourse to methods of cyber warfare certainly would.").

https://doi.org/10.1017/9781108954341.007 Published online by Cambridge University Press

Prosecutor v. *Bemba*, 2016, para. 160), and one can attribute responsibility to particular perpetrators, prove intent, and satisfy jurisdictional requirements. The same cyberattack, if directed toward members of a particular protected group, could additionally constitute the crime against humanity of persecution (see Rome Statute, 1998, Art. 7(1)(h), listing protected groups). Crimes against humanity also include a residual "catch-all" – namely, "[o]ther inhumane acts of a similar character [to other crimes against humanity] intentionally causing great suffering, or serious injury to body or to mental or physical health" (Rome Statute, 1998, Art. 7(1)(k). Cyberattacks with severe consequences, such as a cyber 9/11, could also fall within this category.

While there appears to be great interest and concern about the problem of cyberattacks disrupting elections, to this author such interference – which could certainly be "widespread" *and* "systematic" (although it need not be both) – does not rise to the level of "other inhumane acts" because it would not involve "great suffering, or serious injury to body or to mental or physical health." It also does not appear to fit into any of the other "underlying crimes" of crimes against humanity (see Rome Statute, 1998, Art. 7(1)(a)–(k)).[18]

10 CYBERATTACKS AS GENOCIDE UNDER THE ROME STATUTE

Genocide is a crime that targets members of a distinct "national, ethnical, racial or religious group" (Rome Statute, 1998, Art. 6). For this crime, it is not the attack itself, but the intent behind the attack that is key. The *dolus specialis* (special mental state requirement) of genocide requires proof of: (1) "intent to destroy"; (2) "in whole or in part"; (3) of a "national ethnical, racial or religious group"; and (4) "as such" (i.e., because individuals belong to such a group) (*ibid*.; Kreβ, 2006, p. 498). While genocide includes "inchoate" forms – for example, incitement to commit genocide could be the completed crime (Rome Statute, 1998, Art. 25(3)(e); Ohlin, 2009, discussing "inchoate crimes") – for Rome Statute purposes, if no genocide occurs the crimes probably would not satisfy ICC gravity requirements.

[18] Although some might argue that it could constitute "persecution" against the nationals of another country, that would certainly involve a novel reading of what constitutes persecution, and any ambiguity in Rome Statute crimes, as explained above, must be construed to favor the defense (Rome Statute, 1998, Art. 22(2)). If one does not have an "underlying crime," then pursuant to Article 7(2)(a), the "attack" requirement for crimes against humanity also is not met. Note additionally that as to Russian interference in US elections (see, e.g., Lewis, 2020; Ohlin, 2020), because that involves the territories and nationals of two non-States Parties, there would also be no ICC jurisdiction (see Rome Statute, 1998, Art. 12(2)(a)–(b)), unless, for example, the United States were to enter an Article 12(3) declaration accepting ICC jurisdiction Rome Statute, 1998, Art. 12(3)) – a rather unlikely scenario. By contrast, election interference in various European states (which also has occurred, Apuzzo & Satariano, 2019) who are ICC States Parties would be within ICC jurisdiction as long as an element of the crime occurred in the territory of a State Party (Myanmar/Bangladesh decision, 2019); yet, that is probably moot because this author does not view election interference as meeting the requirements of crimes against humanity (nor any other Rome Statute crime). See discussion below analyzing election interference as a crime of aggression – but concluding it likely also does not meet that definition.

In addition to these overall requirements, there must be "underlying crimes"; the first enumerated being the killing of members of a group (Rome Statute, 1998, Art. 6(a)). The second underlying crime is "[c]ausing serious bodily or mental harm to members of the group" (Rome Statute, 1998, Art. 6(b)). The third underlying crime is "[d]eliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part" (Rome Statute, 1998, Art. 6(c)) – see also Arts. 6(d)–(e)). Again, all are subject to Rome Statute gravity requirements, as one can also imagine a "mental" harm caused by a cyberattack that does not rise to the level of Rome Statute gravity, or creating horrible conditions of life for members of a protected group that is not necessarily aimed at bringing about the group's physical destruction, and/or does not meet Rome Statute gravity. Thus, for a cyberattack to constitute the crime of genocide, it would need to satisfy both this overall special mental state requirement and proof of at least one of the underlying crimes. Additionally, as with all Rome Statute crimes, proof of attribution to particular individuals, proof of intent, and jurisdiction are required.

Here, it may be easier to envision cyber enabled genocide. In Rwanda, in 1994, *Radio Télévision Libre des Mille Collines* (RTLM) was used to incite and facilitate the killing of members of the Tutsi ethnic group – with the Tutsi identified by their government – issued identity cards, particularly at roadblocks (Metzi, 1997). One can similarly imagine cyber means used to compromise hospital or other medical records to identify members of a protected group, and/or; cyber means being used to incite genocide against protected group members (see, e.g., Mozur, 2018, discussing Burmese military Facebook incitement, coupled with crimes against the Rohingya). In either situation, assume the identification of protected group members and/or incitement is followed by killings (as it was in Rwanda and Myanmar), and one could infer the required genocidal intent (see, e.g., *Prosecutor* v. *Akayesu*, 1998); Burmese Military Document entitled "Rohingya Extermination Plan," Mansour, 2017). Either could satisfy the elements of genocide.[19] Roscini also provides the example of a cyberattack that shuts down the cooling system of a nuclear power reactor releasing high levels of radiation killing members of a particular national group, if one could prove genocidal intent (Roscini, 2019, p. 250).

11 CYBERATTACKS AS THE CRIME OF AGGRESSION UNDER THE ROME STATUTE

While the crime of aggression has numerous requirements and warrants a far more extensive discussion (see Trahan, forthcoming), some of the key requirements are that there is a state "act of aggression" (Rome Statute, 1998, Art. 8*bis*, para. 2) that,

[19] The ICC has limited jurisdiction related to crimes against the Rohingya. It only has jurisdiction where one element of the crime occurred in the territory of a Rome Statute State Party (Bangladesh), but not as to crimes committed solely within Myanmar.

to qualify as the crime of aggression, must also constitute a "manifest" violation[20] of the UN Charter by its "character, gravity and scale" (Rome Statute, 1998, Art. 8*bis*, para. 1). The "act of aggression" is defined as "use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations"[21] (Rome Statute, 1998, Art. 8*bis*, para. 2). There is also a list of acts enumerated in Rome Statute Article 8*bis*, paragraph 2 (a)–(g) that could meet that requirement, but each would additionally need to constitute a "manifest" violation of the UN Charter (Rome Statute, 1998, Art. 8*bis*, para. 2 (a)–(g)).[22] Another requirement is that the crime only covers "leaders" in that it applies only to "person[s] in a position effectively to exercise control over or to direct the political or military actions of a State"[23] (Rome Statute, 1998, Art. 8*bis*, para. 1). Also, the leader would need to engage in the "planning, preparation, initiation or execution" of the crime (Rome Statute, 1998, Art. 8*bis*, para. 1).

While the above requirements appear difficult to satisfy, the fourth act enumerated as potentially qualifying as an "act of aggression" is "[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" (Rome Statute, 1998, Art. 8*bis*, para. 2(d)) and Article 8*bis* refers to "the use of *any weapon* by a State against the territory of another State" (Rome Statute, 1998, Art. 8*bis*, para. 2(b) (emphasis added)). Imagine a cyber unit within the armed forces of a state causes weapon systems of the armed forces of another state to become completely inoperable.[24] That would constitute an "attack by the armed forces of a State" on the forces of another state. One would additionally need to attribute responsibility to a particular state leader (or head of cyber command) of the attacking armed forces who is "in a position effectively to exercise control over or to direct the political or military actions of a State," and who planned, prepared, initiated, or played a role in the execution of the cyberattack. Changing the scenario slightly, imagine the leader or head of cyber command instead employs bands of nonstate hackers to conduct the same attack and later acknowledges those acts as acts of the state. Here one would look to the rules

[20] The purpose of the "manifest" requirement is "to exclude minor incidents (e.g., border skirmishes) or legally controversial cases (e.g., a humanitarian intervention) …. (Ambos, 2015, at p. 140).

[21] For analysis of how a cyberattack could constitute the use of "armed force," see Ambos, 2015, at pp. 138–139.

[22] The list of acts of aggression is "open-ended" in that Article 8*bis*, paragraph 2 lists acts that "shall" qualify as acts of aggression, leaving open that other acts might as well. Yet, charging acts not listed might prove risky, as it could run afoul of the principle *nullum crimen sine lege* (no crime without law) and the requirement that ambiguity in the Rome Statute favors the defense (Rome Statute, 1998, Art. 22(2).

[23] For further analysis of the "leadership clause" and its application regarding cyber operations, see Ambos, 2016a.

[24] "[A] cyber operation leaving the targeted object physically intact but neutralizing it in its functionality may amount to a militarily relevant attack." (Ambos, 2015, p. 124, writing this in the context of war crimes).

on state attribution to determine whether the acts of the nonstate actors become attributable to the state, with perhaps the clearest situation being where the hackers are hired into the state cyber command structure, so they become part of the armed forces.[25] In any event, the cyberattack would need to be "manifest," such that it is not *de minimis* (insufficient in gravity and/or scale) and/or "super clear" in terms of its illegality (meeting the required "character"). Yet, because of seemingly extensive jurisdictional limitations – if they are valid (see Trahan, 2018) – it could be quite difficult to trigger ICC jurisdiction regarding the crime of aggression, absent a UN Security Council referral.[26]

Returning to the example of election interference, this author doubts that the elements of the crime of aggression would be satisfied. While election interference could be viewed as a "sovereignty violation" (Shackelford, 2017, 11; Efrony & Shany, 2018, 640), this author does not see it rising to the level of a "manifest" Charter violation, which is required for the crime of aggression (Rome Statute, 1998, Art. 8*bis*, para. 1). Furthermore, at least one significant state involved in election interference, the Russian Federation (Ohlin, 2020), is not a party to the Rome Statute, so there would be no ICC jurisdiction over the crime of aggression committed by Russian nationals (*ibid.*, Art. 15*bis*, para. 5).[27]

12 CONCLUSION

This chapter has briefly touched on what will need to be a far more extensive study considering how the crimes in the ICC's Rome Statute could potentially encompass certain cyberattacks. Yet, hopefully, this chapter has made the case that there is at least some potential for applicability. My forthcoming article and the forthcoming report of the Council of Advisers on the Application of the Rome Statute to Cyberwarfare will expand significantly on these topics.

It is important to engage in this analysis, as there would need to be broad recognition of the ICC's ability to prosecute certain cyberattacks if there is to be any

[25] The International Law Commission in its Articles on State Responsibility for Internationally Wrongful Acts discusses when acts by nonstate actors are attributable to a state (see ILC Articles, 2001, Arts. 5, 8, 9, 11; see also Efrony & Shany, 2018, p. 584; Schmitt 2017, Tallinn 2.0, Rule 14, on attribution).

[26] Absent a UN Security Council referral, if the restrictive interpretation in a certain 2017 Activating Resolution is upheld (ICC, 2017), the ICC would only have jurisdiction over the crime where a State Party that has ratified the Kampala amendment attacks another State Party that has also ratified the Kampala amendment (see Trahan, 2018).

[27] Ironically, this was an exemption that the US delegation negotiated, possibly supported by a few other states, at the ICC Review Conference in Kampala, Uganda (Trahan, 2011). Here, unlike with crimes against humanity, election interference by a non-State Party *even against Rome Statute State Parties* would fall outside ICC jurisdiction (Rome Statute, 1998, Art. 15*bis*, para. 5). Furthermore, due to the veto power of the permanent members of the UN Security Council (UN Charter, Art. 27(3)), one can also anticipate there would be no Security Council referral.

potential for deterrence. Only then can international criminal law in this area play a role in maximizing the potential of reaching a state of cyber peace. It is actually quite significant that there is an existing international criminal tribunal with jurisdiction to prosecute a limited subset of cyberattacks. This capacity was probably never envisioned when the Rome Statute was negotiated; yet, certain cyberattacks appear to meet the elements of the ICC crimes. Whether it is feasible to bring cases will depend if attribution can also be established, and if all of the elements of the crime can be proven through admissible evidence that satisfies the standard, at trial, of proof beyond a reasonable doubt. Perhaps this is not fully feasible now, but as technology develops, it could become more achievable in the future.

None of the cyberattacks perpetrated to date probably have reached the threshold for Rome Statute crimes with the possible exception of those in Ukraine, over which the ICC has an open preliminary examination (ICC, "Preliminary Examination, Ukraine," n.d.). It may also take time for the ICC to develop the required expertise to be able to develop and prosecute such cases, and the ICC may need to rely extensively on the outside expertise of cyber experts. Yet, as mentioned, that also carries potential pitfalls. To the extent the ICC can develop its own internal capacity that could help alleviate potential conflicts of interest.

International criminal law *does* have a role to play here. Will this deter all cyberattackers from committing grievous cyberattacks? The author will not be so naïve to claim that it will. But if the ICC is able to achieve some deterrence – deterring even one horrific cyberattack – that would certainly be a worthwhile endeavor. Ironically, it will be hard to know if such an attack has been deterred, because it would involve the absence of the attack, something notoriously difficult to prove.

While ICC States Parties may be "willing" and "able" to prosecute cyberattacks, and under Article 17 of the Rome Statute, that would then render a case "inadmissible" before the ICC (see Rome Statute, 1998, Art. 17), it is also quite possible that domestic jurisdictions will lack the required laws and/or be unable to exercise jurisdiction over the totality of the crime (which potentially might involve a foreign attacker state and multiple "victim" states). Then, the domestic jurisdiction would be "unable" to prosecute the case fully, likely rendering the case "admissible" before the ICC if other Rome Statute requirements are also satisfied.

To date, most of the ICC's focus has been on crimes in developing countries. Because both developed and developing countries suffer from cyberattacks (probably developed countries even more so), a focus on such crimes before the ICC could be a welcome development, at least in the eyes of many ICC States Parties. Promoting the applicability of the Rome Statute to certain cyberattacks could additionally demonstrate an increased relevance of the ICC to one of the more vexing contemporaneous challenges facing the international community.

REFERENCES

Acquaviva, G. (2014). International criminal courts and tribunals as actors of general deterrence? Perceptions and misperceptions. *International Review of the Red Cross*, *96*(895), 784.

Ambos, K. (2015). International criminal responsibility in cyberspace, in N. Tsagourias & R. Buchan (Eds), *Research handbook on cyberspace and international law*, Edward Elgar, 118.

Ambos, K. (2016a). Individual criminal responsibility for cyber aggression. *Journal of Conflict & Security Law*, *21*(3), 495.

Ambos, K. (2016b). Article 25. Individual criminal responsibility, in O. Triffterer & K. Ambos (Eds), *The Rome Statute of the International Criminal Court: A commentary* (3rd edn, C.H. Beck, Hart, Nomos, 2016), 979.

Apuzzo, M., & Satariano, A. (2019, May 12). Russia Is Targeting Europe's Elections. So Are Far-Right Copycats. *The New York Times*. Retrieved from www.nytimes.com/2019/05/12/world/europe/russian-propaganda-influence-campaign-european-elections-far-right.html

Badar, M. E., & Porro, S. (2017, August 18). Article 30(2)(b), Intent in Relation to Result. *Case Matrix Network*. Retrieved from Case Matrix Network.

Baezner, M., & Robin, P. (2018, January). Hotspot Analysis: Cyber and Information Warfare in the Ukrainian Conflict. CSS Cyber Defense Project.

Bellovin, S. M., Landau, S., & Lin, H. S. (2017). Limiting the undesired impact of cyber weapons: Technical requirements and policy implications. *Journal of Cybersecurity*, *3*(1), 59.

Berger, J. (2016, March 26). A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case. *The New York Times*. Retrieved from www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html

Bezhan, F. (2016, January 5). *Cyberattack on Ukrainian Power Grid Looks to Some Like an Apocalyptic First*. Radio Free Europe. Retrieved from www.rferl.org/a/ukraine-blackout-cyberattack-power-grid-apocalyptic-first/27469154.html

Biller, J. T., & Schmitt, M. N. (2019). Classification of cyber capabilities and operations as weapons, means, or methods of warfare. *International Law Studies*, *95*, 179.

Brenner, J. (2011). *America the vulnerable: Inside the new threat matrix of digital espionage, crime, and warfare*. Penguin Press.

Brierly, J. L. (1944). *The outlook for international law*. Clarendon Press.

Clark, R. S. (2009). Building on article 8(2)(b)(xx) of the Rome Statute of the International Criminal Court: Weapons and methods of warfare. *New Criminal Law Review*, *12*(3), 366.

Cross, M. E. (2020). Strategising international prosecutions: How might the work of the Kosovo specialist prosecutor's office come to be judged? *International Criminal Law Review*, *20*(1), 43.

Decision Pursuant to Article 15 of the Rome Statute on the Authorisation of an Investigation into the Situation in the People's Republic of Bangladesh/Republic of the Union of Myanmar, Case No. ICC-01/19-27, Judgment, ¶ 61 (November 1, 2019) ("Myanmar/Bangladesh decision, 2019").

Dederer, H-G., & Singer, T. (2019). Adverse cyber operations: Causality, attribution, evidence, and due diligence. *International Law Studies*, *95*(1), 430.

deGuzman, M. M. (2020). *Shocking the conscience of humanity: Gravity and the legitimacy of international criminal law*. Oxford University Press.

Droit International Appliqué aux Opérations dans le Cyberspace. (2019). Just Security. Retrieved from www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqu%C3%A9-aux-op%C3%A9rations-cyberespace-france.pdf

https://doi.org/10.1017/9781108954341.007 Published online by Cambridge University Press

Efrony, D., & Shany, Y. (2018). A rule book on the shelf? Tallinn manual 2.0 on cyber operations and subsequent state practice. *American Journal of International Law*, *112*(4), 583.
Eichensehr, K. (2020). The law & politics of cyberattack attribution. *UCLA Law Review*, *67*, 520.
Geneva Convention I for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (1949, August 12). 75 UNTS 31. Geneva Convention II for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea. (1949, August 12). 75 UNTS 85. Geneva Convention III Relative to the Treatment of Prisoners of War. (1949, August 12). 75 UNTS 135. Geneva Convention IV Relative to the Protection of Civilian Persons in Time of War. (1949, August 12). 75 UNTS 287. (Collectively, "1949 Geneva Conventions").
Glaser, A. (2017, June 27). *U.S. Hospitals Have Been Hit by the Global Ransomware Attack*. Vox. Retrieved from www.vox.com/2017/6/27/15881666/global-eu-cyberattack-us-hackers-nsa-hospitals
Greenberg, A. (2018, August 22). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. Retrieved from www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
Greenberg, A. (2017a, July 6). Hack Brief: Hackers Targeted a US Nuclear Plant (But Don't Panic Yet). *Wired*. Retrieved from www.wired.com/story/hack-brief-us-nuclear-power-breach/#intcid=recommendations_wired-bottom-recirc-similar_1691318a-b422-4428-96db-e7512a834566_text2vec1_text2VecSimilarity
Greenberg, A. (2017b, September 6). Hackers Gain Direct Access to US Power Grid Controls. *Wired*. Retrieved from www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/#intcid=recommendations_wired-bottom-recirc-similar_712531e1-69ed-4994-b83b-891af026859f_text2vec1_text2VecSimilarity
Greenfield, R. (2013, April 23). Look What the Hacked AP Tweet About White House Bombs Did to the Market. *The Atlantic*. Retrieved from www.theatlantic.com/technology/archive/2013/04/hacked-ap-tweet-white-house-bombs-stock-market/315992/
Griffiths, J. (2015, October 8). Cybercrime Costs the Average U.S. Firm $15 Million a Year. *CNN Tech*. Retrieved from https://money.cnn.com/2015/10/08/technology/cybercrime-cost-business/
Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Speigel, J. (2012). The law of cyber attack. *California Law Review*, *100*(4), 817.
Hillebrecht, C. (2016). The deterrent effects of the international criminal court: Evidence from Libya. *International Interactions*, *42*(4), 616.
Horowitz, J. (2020, May 19). Cyber operations under international humanitarian law: Perspectives from the ICRC. *ASIL Insights*, *24*(11).
Human Rights Watch. (2009, July 7). *Selling Justice Short, Why Accountability Matters for Peace*. HRW. Retrieved from www.hrw.org/en/node/84262/section/2
ICC. (2011). *Elements of Crimes*. Retrieved from www.icc-cpi.int/resource-library/Documents/ElementsOfCrimesEng.pdf
ICC. (n.d.). *Preliminary Examination, Ukraine*. Retrieved from www.icc-cpi.int/ukraine#:~:text=On%2025%20April%202014%2C%20the,in%20Crimea%20and%20eastern%20Ukraine
ICC. (n.d.). *States Parties, Chronological List*. Retrieved from https://asp.icc-cpi.int/en_menus/asp/states%20parties/Pages/states%20parties%20_%20chronological%20list.aspx
ICC. (n.d.). *Warrant/Summonses*. Retrieved from www.icc-cpi.int/cases#Default=%7B%22k%22%3A%22%22%7D#2ae8b286-eb20-4b32-8076-17d2a9d9a00e=%7B%22k%22%3A%22%22%7D

https://doi.org/10.1017/9781108954341.007 Published online by Cambridge University Press

ICC Forum. (2018, February 22). New Frontiers for the ICC (International Criminal Court): Tackling Cyber Attacks through the Crime of Aggression. Retrieved from https://iccforum.com/forum/permalink/110/13832

Int'l L. Comm'n. (2001). Draft Articles on the Responsibility of States for Internationally Wrongful Acts, with Commentaries (adopted). UN Doc. A/56/10. ("ILC Articles").

International Criminal Court. (2017, December 14). Activation of the Jurisdiction of the Court Over the Crime of Aggression. Retrieved from https://asp.icc-cpi.int/iccdocs/asp_docs/Resolutions/ASP16/ICC-ASP-16-Res5-ENG.pdf

Jensen, E. T. (2017). The Tallinn manual 2.0: Highlights and insights. *Georgetown Journal of International Law*, *48*, 735.

Jo, H., & Simmons, B. A. (2016). Can the International Criminal Court deter atrocity? *International Organization*, *70*(3), 443.

Kampala amendment. (2010, June 2011, adopted by consensus). RC/Res.6*. Review Conference of the Rome Statute. Retrieved from https://treaties.un.org/doc/source/docs/RC-Res.6-ENG.pdf

Koh, H. H. (2012). International law in cyberspace. *Harvard International Law Journal Online*, *54*, 1.

Kreβ, C. (2006). The crime of genocide under international law. *International Criminal Law Review*, *6*(4), 461.

Lewis, J. (2020, February 4). *Election Interference and the Emperor's New Clothes*. Center for Strategic & International Studies. Retrieved from www.csis.org/analysis/election-interference-and-emperors-new-clothes?gclid=EAIaIQobChMI5vfYtZ-36wIVgP3jBx-3YLArAEAAYASAAEgKN-fD_BwE

Mačák, K. (2015). Military objectives 2.0: The case for interpreting computer data as objects under international humanitarian law. *Israel Law Review*, *48*(1), 55.

Mačák, K. (2019). On the shelf, but close at hand: The contribution of non-state initiatives to international cyber law. *AJIL Unbound*, *113*, 81.

Mačák, K., Gisel, L., & Rodenhäuser, T. (2020, March 27). *Cyber Attacks against Hospitals and the COVID-19 Pandemic: How Strong Are International Law Protections?* Just Security. Retrieved from www.justsecurity.org/69407/cyberattacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/

Mansour, H. (2017, January 10). *The 1988 Rohingya Extermination Blueprint*. Human Rights for All. Retrieved from https://merhrom.wordpress.com/2017/01/10/the-1988-rohingya-extermination-blueprint/

McAllister, J. R. (2019–20). Deterring wartime atrocities: Hard lessons from the Yugoslav tribunal. *International Security*, *44*(3), 84.

Metzi, J. F. (1997). Rwandan genocide and the international law of radio jamming. *American Journal of International Law*, *91*(4), 628–651.

Mozur, P. (2018, October 15). A Genocide Incited on Facebook, with Posts from Myanmar's Military. *The New York Times*. Retrieved from www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html

O'Hare, R. (2016, November 1). China Proudly Debuts Its New Stealth Jet It Built 'by Hacking into US Computers and Stealing Plans.' *Daily Mail*. Retrieved from www.dailymail.co.uk/sciencetech/article-3893126/Chinese-J-20-stealth-jet-based-military-plans-stolen-hackers-makespublic-debut.html

Ohlin, J. D. (2009). Attempt, Conspiracy, and Incitement to Commit Genocide. *Cornell Law Faculty Publications*, Paper 24.

Ohlin, J. D. (2020). *Election interference: International law and the future of democracy*. Cambridge University Press.

https://doi.org/10.1017/9781108954341.007 Published online by Cambridge University Press

OTP. (2017, December 4). Report on Preliminary Examination Activities (2017) – Registered Vessels of Comoros, Greece and Cambodia. *International Criminal Court*. Retrieved from www.icc-cpi.int/Pages/item.aspx?name=2017-otp-rep-PE-Comoros

The Council of Advisers. (2021). Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare. Retrieved from 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

The Paris Call for Trust and Security in Cyberspace. (2018, November 12). The Paris Call. Retrieved from https://pariscall.international/en/call

Policy Paper on Preliminary Examinations. (2013, November). *International Criminal Court*. Retrieved from www.icc-cpi.int/iccdocs/otp/otp-policy_paper_preliminary_examinations_2013-eng.pdf

Prosecutor v. *Akayesu*, Case No. ICTR-96-4, Judgment (September 2, 1998).

Prosecutor v. *Ahmad Al Faqi Al Mahdi*, Case Information Sheet. ICC-01/12-01/15. Retrieved from www.icc-cpi.int/CaseInformationSheets/al-mahdiEng.pdf

Prosecutor v. *Al Hassan*, Case No. ICC-01/12-01/18-601-Red OA, Judgment on the appeal of Mr. Al Hassan against the decision of Pre-Trial Chamber I entitled '*Décision relative à l'exception d'irrecevabilité pour insuffisance de gravité de l'affaire soulevée par la defense*' (February 19, 2020).

Prosecutor v. *Bemba*, Case No. ICC-01/05-01/08-424, Decision Pursuant to Article 61(7) (a) and (b) of the Rome Statute on the Charges of the Prosecutor Against Jean-Pierre Bemba Gombo (June 15, 2009).

Prosecutor v. *Bemba*, Case No. ICC-01/05-01/08, Judgment (March 21, 2016).

Prosecutor v. *Lubanga*, Case No. ICC-01/04-01/06-A-5, Judgment on the Appeal of Mr. Thomas Lubanga Dyilo against his conviction (December 1, 2014).

Prosecutor v. *Ntaganda*, Case No. ICC-01/04-02/06, Judgment (July 8, 2019). Retrieved from www.icc-cpi.int/CourtRecords/CR2019_03568.PDF

Prosecutor v. *Tadić*, Case No. IT-94-IAR72, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction (October 2, 1995) ("Tadić case").

Rome Statute of the International Criminal Court. (1998, July 17). UN Doc. A/CONF.183/9*. As amended.

Rona, G. (2003). Interesting times for international humanitarian law: Challenges from the "War on Terror." *The Fletcher Forum on World Affairs*, 27(2), 55.

Roscini, M. (2019). Gravity in the statute of the International Criminal Court and cyber conduct that constitutes, instigates or facilitates international crimes. *Criminal Law Forum*, 30(3), 247.

Rowe, N. C. (2007). War crimes from cyberweapons. *Journal of Information Warfare*, 6(3), 15. Retrieved from https://faculty.nps.edu/ncrowe/iwcrimes.htm

Schense, J., & Carter, L. (Eds). (2017). *Two steps forward, one step back: The deterrent effect of international criminal tribunals*. Torkel Opsahl Academic EPublisher.

Schmitt, M. N. (Ed.). (2017, 2nd edn). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Schmitt, M. N. (2019, September 16). France's Major Statement on International Law and Cyber: An Assessment. *Just Security*. Retrieved from www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/

Shackelford, S. J. (2017). The law of cyber peace. *Chicago Journal of International Law*, 18(1), 1.

Statute of the Special Court for Sierra Leone. Retrieved from www.rscsl.org/Documents/scsl-statute.pdf. ("Special Court Statute").

Stubbs, J., & Bing, C. (2019, October 21). Hacking the Hackers: Russian Group Hijacked Iranian Spying Operation, Officials Say. *Reuters*. Retrieved from www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1X00AK

Trahan, J. (2011). The Rome Statute's amendment on the crime of aggression: Negotiations at the Kampala review conference. *International Criminal Law Review*, *11*(1), 49.

Trahan, J. (2018). From Kampala to New York—The final negotiations to activate the jurisdiction of the International Criminal Court over the crime of aggression. *International Criminal Law Review*, *18*(2), 197.

Trahan, J. (2021). International justice and the International Criminal Court at a critical juncture, in C. Ankersen & W. P. S. Sidhu (Eds.), *The future of global affairs: Managing discontinuity, disruption and destruction*. Palgrave Macmillan.

Trahan, J. (*Forthcoming*). The criminalization of cyberattacks under the International Criminal Court's Rome Statute. *Journal of International Criminal Justice*.

Tsagourias, N. (2012). Cyber attacks, self-defense and the problem of attribution. *Journal of Conflict & Security Law*, *17*(2), 229.

UK Government. (2018, May 23). *Cyber and International Law in the 21st Century*. Retrieved from www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

UN Charter. (1945, October 24). 1 UNTS XVI.

UN GGE and OEWG. (n.d.). Digital Watch. Retrieved from https://dig.watch/processes/un-gge

U.N. Security Council. (2005, March 31). U.N. Security Council Resolution 1593, U.N. Doc. S/RES/1593.

U.N. Security Council. (2011, February 26). U.N. Security Council Resolution 1970, U.N. Doc. S/RES/1970.

United Nations Treaty Collection. (As of 2020, August 7). Ch. XVIII. Penal Matters. Amendments on the crime of aggression to the Rome Statute of the International Criminal Court. Retrieved from https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-10-b&chapter=18&lang=en ("States Parties to the Kampala amendment")

U.S. Department of Homeland Security, CISA Cyber & Infrastructure. (Last revised 2019, November 20). *Understanding Denial-of-Service Attacks*. CISA. Retrieved from www.us-cert.gov/ncas/tips/ST04-015

Warrell, H., Seddon, M., & Manson, K. (2020, February 20). Russia Military Unit Accused of Georgia Cyber Attacks. *Financial Times*. Retrieved from www.ft.com/content/14377b84-53e3-11ea-90ad-25e377c0ee1f

Whiting, A. (2015, July 20). *The ICC Prosecutor Should Reject Judges' Decision in Mavi Marmara*. Just Security. Retrieved from www.justsecurity.org/24778/icc-prosecutor-reject-judges-decision-mavi-marmara/