THE COUNCIL OF ADVISERS' REPORT ON THE APPLICATION OF THE ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT TO CYBERWARFARE

PREPARED BY THE
PERMANENT MISSION OF LIECHTENSTEIN
TO THE UNITED NATIONS

The Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare

Prepared by the Permanent Mission of Liechtenstein to the United Nations

August 2021

This report is based on a series of three convenings involving a group of eminent legal and technical experts across 2019 and 2020 to discuss the extent to which the Rome Statute's core provisions apply to cyberwarfare. The convenings were hosted by the Permanent Mission of Liechtenstein to the United Nations, and co-organized by the Permanent Missions of 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 (GIPA). The Harvard Law School Program on International Law and Armed Conflict (HLS PILAC) and the UCLA School of Law International Human Rights Law Association also contributed independent legal research, through the provision of students' assistance for the report's preparation.

CONTENTS

LIST OF PARTICIPANTS

Members of the Council of Advisers, experts in the laws on the use of force and cyberwarfare, were invited to join three in-person consultations and contributed to the final report.

The list of members of the Council of Advisers is as follows:

- ***Convenor:*** Don Ferencz, Founder of the Global Institute for the Prevention of Aggression
- ***Chair:*** Christian Wenaweser, Ambassador, Permanent Representative of Liechtenstein to the United Nations
- ***Council of Advisers*:**
  - Roger Clark, Rutgers Law School
  - Rebecca Crootof, University of Richmond Law School
  - Pedro Pérez Enciso, Prosecutor, Eurojust National Coordinator, Spain
  - Claire Finkelstein, University of Pennsylvania Law School
  - Oona Hathaway, Yale Law School
  - Charles C. Jalloh, Florida International University, College of Law
  - Jocelyn Getgen Kestenbaum, Benjamin N. Cardozo School of Law
  - Claus Kreß, University of Cologne
  - Markko Kunnapu, e-Governance Academy, Estonia
  - Kate Mackintosh, UCLA School of Law
  - Frédéric Megret, McGill University
  - Jens David Ohlin, Cornell Law School
  - Scott Shapiro, Yale Law School
  - Jennifer Trahan, New York University Center for Global Affairs
  - Noah Weisbord, Queen's University Faculty of Law
- ***Project Director and Managing Editor:*** Sina Alavi, Legal Adviser, Permanent Mission of Liechtenstein to the United Nations
- ***Assistant Editor:***
  - Shira Shamir
- ***Legal Researchers:***
  - Brady Mabe
  - Kritika Sharma

- ***Legal Assistants:***
  - Eszter Boldis
  - Leigh Marie Dannhauser
  - Aya Dardari
  - William Edin
  - Nelly Gordpour
  - Alex Gulino
  - Lina Jemili
  - Sam Lusher
  - Amy McMeeking
  - Fatima Mehmood
  - Fraciah Muringi Njoroge
  - Tamsin Parzen
  - Heebum Shin
  - Richard Spronz
- ***Technical Experts:***
  - Marcus Comiter, Harvard Kennedy School's Belfer Center
  - Lauri Tankler, Estonian Information System Authority
  - Pano Yannakogeorgos, New York University Center for Global Affairs
- ***Project Assistant:***
  - Diana Barnes
- ***Other participants:***
  - Matthew Cross, Office of the Prosecutor, International Criminal Court
  - Christopher Harland, International Committee of the Red Cross

FOREWORD

CHRISTIAN WENAWESER

Permanent Representative of Liechtenstein to the United Nations

The application of the rule of law is of paramount importance for the maintenance of international peace and security. The advent of new cyber technologies in today's interconnected world not only offers unprecedented opportunities for international cooperation, but also presents the risk of malicious cyber operations with potentially disastrous effects. Such cyber operations have the potential to inflict grave suffering on civilians, yet there is a dearth of discussion about how international criminal law applies to cyberwarfare. There is broad agreement that international law generally applies to cyberspace, but no consensus regarding its application in practice.

This report intends to contribute to developing a clearer understanding of how the Rome Statute of the International Criminal Court applies in the cyber context. Such clarity is necessary for the Court's own work, but it can also help inform the work of the United Nations Security Council, in particular regarding how it uses its power to refer situations involving acts of aggression to the ICC – a referral power that provides an important enforcement mechanism in support of the UN Charter's prohibition on the use of force.

International peace and security depend on how prepared we are to address foreseeable threats. We should be ready for the potential wars of the 21st century by deterring malicious cyber operations through establishing the necessary means for accountability.

FOREWORD

BENJAMIN FERENCZ

Former Nuremberg Trials Prosecutor

Preventing armed conflict was a core objective of those who drafted the Charter of the United Nations, and the general prohibition of the use of force became a cornerstone of the UN Charter. Bringing illegal war-making under the jurisdiction of a permanent international criminal court was the element we were missing for too long. Never has humanity had a permanent international court with the authority to hold individuals accountable for their decisions to commit aggression. Now we do. But more work remains to be done. While the International Criminal Court, since 2018, has jurisdiction over the crime of aggression, we must work to make sure it is applied. In particular, I have warned for years that malicious cyber operations have tremendous power to destroy. It is thus crucial to prevent such warfare while preparing for the possible reality of the gravest iterations of its implementation.

Nuremberg prosecutors, myself included, tried and convicted perpetrators of crimes against peace, war crimes and crimes against humanity. Many of the Nuremburg defendants argued that they were acting in preemptive self-defense — the very argument that some actors try to use today. We need to change our understanding of illegal war-making, making it unacceptable by any means, in any situation. We must continue to build on the Nuremberg legacy and the progress of the ICC to strengthen the rule of law through a more effective and robust international criminal legal system. We must never stop working together toward a world ruled by law, not war.

INTRODUCTION

The notion that a limited subset of malicious cyber operations could constitute crimes under the Rome Statute of the International Criminal Court (ICC) could potentially contribute to deterring such crimes. Malign cyber operations – which have become an unfortunate and nearly daily occurrence – do not occur in a law-free domain but are subject to various bodies of international law, including the Rome Statute. Realizing this potential of the Rome Statute means such crimes could currently be prosecutable at the ICC (subject to jurisdictional and other requirements), without the need for any statutory amendment. Increased awareness of the ICC's ability to prosecute such crimes could demonstrate an additional relevance of the world's only permanent international criminal court to address this significant contemporaneous challenge, one that plagues developed and developing countries alike. The Tallinn Manual, which has been at the center of the discussion in the emerging field of international cyber law, falls short of addressing the specific application of the Rome Statute. This report focuses on how each of the Rome Statute crimes can be applied to cyberwarfare. This is an area of the law that can undoubtedly benefit from greater understanding and clarity. It is therefore encouraged that others, not least governments, make public their interpretations of how the Rome Statute, and international criminal law more broadly, apply to cyberwarfare.

Cyber operations have moreover served as the equalizer in modern warfare by providing new avenues for both offensive and defensive operations to actors with fewer resources. As a result, the frequency and severity of cyber operations have intensified in recent years. Ensuing attacks on major national infrastructure and government agencies by ransomware demonstrate the grave implications of cyber operations by state and non-state actors in times of war and peace. In particular, cyber operations have the potential to cause grave suffering of the civilian population, including suffering equal to that caused by the most serious crimes of international concern in the Rome Statute: genocide, crimes against humanity, war crimes, and crimes of aggression.

Given that the Rome Statute was drafted at the early stages of global digitalization, uncertainty due to the dearth of established legal instruments and precedents under international criminal law gives rise to numerous legal questions about cyberwarfare. For example, what if a State takes control of a dam through ransomware and opens its gates, resulting in countless

civilian casualties downstream? Could the nationals of that State be held accountable under the Rome Statute? If so, which crime(s) would the cyber operation fall under? In another scenario, similar questions may arise when a terrorist organization, state-sponsored or not, uses cyber operations to shut down the cooling system in a nuclear power plant, causing the release of radioactive materials and resulting in the death of civilians living near the plant. This report seeks to answer such questions regarding the applicability of the Rome Statute to cyber operations.

The question of what role the ICC may play in the regulation of warfare as it evolves in the 21st century led to the creation of the Council of Advisers on the Application of the Rome Statute to Cyberwarfare ("Council of Advisers" or "Council"). The Council was composed of 15 international lawyers and assisted by three technical experts, as well as one representative of the International Committee of the Red Cross and one representative of the Office of Prosecutor of the ICC. The Council was convened three times during 2019 and 2020. The first convening in October 2019 discussed the issues of constructive ambiguity in the list of acts of aggression, "manifest" violations of the UN Charter, "armed" attacks, and non-state actors. The second convening in December 2019 focused on use-of-force thresholds, proportional responses, the "leadership requirement," and Kampala-related jurisdictional issues for cyber operations. The third convening in January 2020 covered cyberwarfare and the Rome Statute beyond the Kampala amendments on the crime of aggression. This report consolidates the discussions of the Council of Advisers during the three abovementioned convenings and subsequent email exchanges.[*]

Although various discussions on the application of international law to cyber operations have occurred and continue to take place in different fora, this report's contribution is in its specific and unique focus on the application of the Rome Statute of the ICC to cyber operations. The report discusses the crime of aggression in Part I, war crimes in Part II, crimes against humanity in Part III, and genocide in Part IV. Each part introduces relevant provisions and discusses specific points at issue within those provisions. It should be noted that the order followed in this report reflects the Council's view regarding the applicability of the crimes in the

[*] The Advisers participated in a series of conversations that formed the basis for this report. Not every Adviser participated in every conversation and therefore not every Adviser necessarily contributed to or endorses the entirety of the report.

Rome Statute; the link of the crime of aggression to cyber operations may be more obvious than genocide. It is also important to note that the Council did not envision its role as an arbiter of every Rome Statute issue related to cyber operations, but as an initiator of further discussion regarding how international criminal law applies to cyber operations.

The nature of cyber operations presents unique considerations and challenges, namely with regard to intent and responsibility. A cyber operation may have seemingly unintentional or unpredictable consequences due to the complexity of the technologies used and their spillover effects, making it difficult to infer the intent behind the particular act with regard to responsibility. Furthermore, cyber operations are notoriously difficult to attribute. States may attempt to disguise their cyber activities or may outsource cyber activities to "black-hat hackers," who can be difficult to individually trace and even more difficult to link back to State officials giving orders. Some cyber operations may involve multiple actors. Difficulties in attributing a crime not just to a state or non-state actor, but to particular perpetrators present further challenges for prosecutors to meet the ICC's evidentiary standard of proof beyond a reasonable doubt. These challenges exist in the context of each of the crimes enumerated in this report.

Despite these challenges, the Council agreed that exploring the application of the Rome Statute to cyber operations would be crucial in establishing and enforcing accountability for perpetrators of such crimes. The Council hopes that an increased understanding and awareness of the potential of the Rome Statute with respect to the prosecution of relevant cyber operations can contribute to deterring such crimes and bringing justice to victims.

PART I

The Application of Articles 8*bis*, 15*bis*, and 15*ter* (Crime of Aggression) of the Rome Statute to Cyberwarfare

PART I: THE APPLICATION OF ARTICLE 8*BIS*, ARTICLE 15*BIS*, AND ARTICLE 15*TER* (CRIME OF AGGRESSION) OF THE ROME STATUTE TO CYBERWARFARE

SECTION I

The Crime of Aggression in the International Criminal Court: General Overview

The crime of aggression is defined in Article 8*bis* of the Rome Statute, while Articles 15*bis* and 15*ter* govern the ICC's jurisdiction over this crime.[1] Article 8*bis* sets out that a crime of aggression is committed when a political or military leader of a State causes (through planning, preparation, initiation, or execution) that State to illegally use force against another State, provided that the use of force constitutes by its character, gravity, and scale a manifest violation of the United Nations Charter. This implies that only the most serious forms of illegal use of force between States can be subject to the ICC's jurisdiction. Cases of lawful individual or collective self-defense, as well as action authorized by the UN Security Council are thus excluded.[2] Since activation of the Court's jurisdiction over the crime of aggression on 17 July 2018, the possibility for criminal accountability at the international level for this "supreme crime"[3] exists. The most important steps that led to this development, beginning with the entry into force of the Charter of the United Nations, are summarized below to provide the necessary broader context of the discussions that took place among the members of the Council of Advisers with respect to the crime of aggression.

---

[1] *See* THE CRIME OF AGGRESSION: A COMMENTARY (Claus Kreß & Stefan Barriga eds., 2016). *See also* Carrie McDougall, THE CRIME OF AGGRESSION UNDER THE ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT (2 ed. 2021).

[2] Whether something that resembles "*bona fide*" "humanitarian intervention" (to the extent that concept exists) is implicitly also excluded involves a complex discussion that is beyond the scope of the present report. For one view, *see* Jennifer Trahan, *Defining the 'Grey Area' Where Humanitarian Intervention May Not Be Fully Legal, but Is Not the Crime of Aggression*, 2 J. ON USE OF FORCE & INT'L L. 42 (2015).

[3] United States v. Göring, Judgment, *in* TRIAL OF THE MAJOR WAR CRIMINALS BEFORE THE INTERNATIONAL MILITARY TRIBUNAL 186 (1947).

The United Nations Charter and the Nuremberg and Tokyo Trials (1945–48)[4]

On 24 October 1945, the United Nations Charter entered into force, thus establishing a system of collective security. Article 2(4) of the Charter prohibits the "threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations."[5] The Charter expressly allows the use of force only for the purpose of lawful individual or collective self-defense or upon authorization by the Security Council.[6] The Charter mandates the Security Council to respond to threats to the peace, breaches of the peace, and acts of aggression. It does not, however, define the notion of aggression, nor does it provide for individual criminal accountability in cases of aggression.

The victorious powers of World War II conducted trials in Nuremberg (1945–46) and Tokyo (1946–48) to prosecute those most responsible for crimes against peace, war crimes, and crimes against humanity. The Nuremberg Charter defined crimes against peace as "planning, preparation, initiation or waging of a war of aggression, or a war in violation of international treaties, agreements or assurances, or participation in a Common Plan or Conspiracy for the accomplishment of the foregoing."[7] It did not, however, specify further what was meant by "aggression," and the International Military Tribunal at Nuremberg was left to fill it in through judicial construction. Conspiracy to commit aggression was the linchpin of the prosecution's case at Nuremberg, linking individual defendants to mass crimes spanning many countries.[8] Subsequent to the Nuremberg trial, the UN General Assembly affirmed the principles of the Nuremberg Charter and the Nuremberg Tribunal's judgment in Resolution 95(I).[9]

---

[4] *See* KIRSTEN SELLARS, 'CRIMES AGAINST PEACE' AND INTERNATIONAL LAW (2013).

[5] U.N. Charter art. 2, ¶ 4.

[6] *Id.* art. 51.

[7] Agreement for the Prosecution and Punishment of the Major War Criminals of the European Axis art. 6(a), Aug. 8, 1945, 82 U.N.T.S 279 [hereinafter Nuremberg Charter].

[8] NOAH WEISBORD, *The Nuremberg Avant-Garde Moment*, *in* THE CRIME OF AGGRESSION: THE QUEST FOR JUSTICE IN AN AGE OF DRONES, CYBERATTACKS, INSURGENTS, AND AUTOCRATS 49 (2019).

[9] G.A. Res 95 (I), (Dec. 11, 1946).

The General Assembly Definition (1974)[10]

In December 1974, following decades of negotiations, the UN General Assembly adopted Resolution 3314 (XXIX).[11] The purpose of the definition of aggression annexed to the Resolution was to give guidance to the Security Council in its determination of the existence of an act of aggression. Notably, the definition deals with the State act of aggression, not the act of an individual who may be responsible for the State act. The definition of aggression essentially mirrors the notion of the illegal use of force contained in Article 2(4) of the Charter and enumerates specific examples of acts of aggression, such as the invasion or attack by the armed forces of a State of the territory of another State (including related military occupation), bombardment by the armed forces of a State against the territory of another State, etc. The core provisions of the 1974 definition (Articles 1 and 3) were later incorporated into part of the 2010 definition of the crime of aggression under the Rome Statute.

The Rome Conference (1998)

The question of whether to include the crime of aggression—and if so, how to define it—was one of the central disputes at the July 1998 diplomatic conference that led to the adoption of the Rome Statute. Delegates could not agree on a definition of the crime of aggression, as some wanted only "wars of aggression" to be covered, whereas others wanted to use what is arguably the broader notion of "acts of aggression" contained in the 1974 General Assembly definition.[12] Even more difficult was the question of whether the ICC should only prosecute crimes of aggression once the Security Council determined the existence of an act of aggression by one State against another.[13] As part of the final compromise, the crime of aggression was included in the list of crimes under the jurisdiction of the Court, but the definition and the conditions for the exercise of jurisdiction (including the question of the role of the Security Council) were deferred for consideration at the first ICC Review Conference.

---

[10] *See* THOMAS BRUHA, *The General Assembly's Definition of the Act of Aggression*, *in* THE CRIME OF AGGRESSION: A COMMENTARY 142–177 (Claus Kreß & Stefan Barriga eds., 2016).

[11] G.A. Res 3314 (XXIX), (Dec. 14, 1974).

[12] Roger S. Clark, *Negotiations on the Rome Statute, 1995–98*, *in* THE CRIME OF AGGRESSION: A COMMENTARY 244–270 (Claus Kreß & Stefan Barriga eds., 2016).

[13] U.N. Charter art. 39.

The Kampala Review Conference (2010)

Following the 1998 Rome Conference, the Preparatory Commission for the ICC (PrepComm, 1999–2002) and later the Special Working Group on the Crime of Aggression (SWGCA, 2003–09) continued negotiations on the outstanding issues regarding the crime of aggression.[14] In February 2009, the SWGCA arrived at a consensus agreement on the definition of the crime of aggression. The 2010 Kampala Review Conference used that definition and could thus focus on other outstanding issues, i.e., the conditions for the exercise of jurisdiction. States Parties seized the historic opportunity and adopted Resolution RC/Res.6 by consensus.[15] The resolution amended the Rome Statute to include, inter alia, a new Article 8*bis* containing the definition of the crime of aggression and new Articles 15*bis* and 15*ter*, containing complex provisions on the conditions for the exercise of jurisdiction. Notably, the compromise included a clause that prevented the Court from exercising jurisdiction over the crime of aggression immediately. Instead, the Assembly of States Parties (ASP) had to make a further one-time decision to activate the Court's jurisdiction, no earlier than 2017, and the Court could not exercise its jurisdiction until a year after the 30th ratification of the crime of aggression amendment.[16]

The Sixteenth Session of the ICC Assembly of States Parties (2017)

On 14 December 2017, 123 States Parties to the Rome Statute made the historic decision to enable the ICC to prosecute the crime of aggression by adopting Resolution ICC-ASP/16/Res.5 by consensus.[17] The Court's

---

[14] *See* C. Kreß & L. von Holtzendorff, *The Kampala Compromise on the Crime of Aggression*, 8 J. OF INT'L CRIM. JUSTICE 1179–1217 (2010).

[15] International Criminal Court, Assembly of States Parties, Review Conference, ICC Doc. RC/Res.6, *The Crime of Aggression* (June 11, 2010) [hereinafter Kampala Amendments].

[16] Rome Statute of the International Criminal Court, art. 15*bis*(2), July 17, 1998, 2187 U.N.T.S. 90 [hereinafter Rome Statute]. Palestine was the thirtieth State Party to ratify the Kampala amendments on 26 June 2016. The majority of NATO members have ratified the amendments. *See Amendments on the Crime of Aggression to the Rome Statute of the International Criminal Court*, UNITED NATIONS TREATY COLLECTION, https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-10-b&chapter=18&clang=_en (last visited August 2, 2021).

[17] International Criminal Court [ICC], Assembly of States Parties, Resolution ICC-ASP/16/Res.5, *Activation of the jurisdiction of the Court over the crime of aggression.* (Dec. 14,

jurisdiction over the crime of aggression subsequently went into effect on 17 July 2018, which also marked the 20th anniversary of the Rome Statute. For the first time ever, humanity has a permanent international court with the authority to hold individuals accountable for committing the most serious forms of the illegal use of force. The decision to activate the ICC's jurisdiction over the crime of aggression not only completed the Rome Statute as originally drafted, but also reinforces the Charter of the United Nations by helping to deter aggressive war-making, not least because of the power of the Security Council to refer aggression situations to the ICC. The Court's jurisdiction over the crime of aggression has the potential to play an important role in the regulation of warfare, in particular cyberwarfare, as it continues to evolve in the 21st century.

SECTION II

The following section reflects the Council of Advisers' discussion on when cyber operations may constitute the crime of aggression as set out in Article 8*bis* of the Rome Statute.

The Nature of the List of Acts of Aggression Enumerated in Article 8*bis*

The use of "armed force" element for an act of aggression applies regardless of the specific weapon used, whether conventional or cyber.

1. Article 8*bis*(2) defines an "act of aggression" as the "the use of armed force by a state against the sovereignty, territorial integrity or political independence of another state." It then goes on to list seven acts which qualify as aggression. This list is taken unaltered from Article 3 of the United Nations General Assembly Resolution 3314 (1974).[18] This list captures how aggression has been understood and seen, ranging from archetypal invasions,

---

2017) [hereinafter Resolution ICC-ASP/16/Res.5]. *See also* Claus Kreß, *On the Activation of ICC Jurisdiction over the Crime of Aggression*, 16 J. OF INT'L CRIM. JUSTICE 1–17 (2018).

[18] G.A. Res. 3314, *supra* note 11.

military occupations, annexations[19] to bombardments,[20] blockades,[21] sending of armed mercenaries[22] and nations allowing their territories to be used by other States to invade third States.[23]

2. In discussing the meaning of the word "armed," the Council of Advisers agreed that any use of force regardless of the specific weapon used, would satisfy the use of "armed force" element for what constitutes an act of aggression under Article 8*bis*. The International Court of Justice in its advisory opinion about nuclear weapons makes clear that use of force may be accomplished "regardless of the weapons employed."[24] There is no reason to treat the situation differently from equivalent attacks conducted through kinetic methods of warfare.
3. The Council of Advisers noted that cyberwarfare does not fit into traditional kinetic, state-centric, territory-focused notions of acts of aggression. Yet, the Council concluded that there are two ways in which cyber operations could fit into the specific list of acts of aggression enumerated in Article 8*bis* of the Rome Statute. First, the list is not exhaustive. Second, many of the acts in the list can be interpreted to apply to cyber operations, subject to the provisions of Article 22(2) of the Rome Statute, which stipulates that "the definition of a crime shall be strictly construed and shall not be extended by analogy". [25] Some acts clearly lend themselves to such interpretation more easily than others.
4. The Council of Advisers agreed that Article *8bis* in fact encapsulates a non-exhaustive list of acts amounting to acts of aggression, as the list allows the ICC to find other uses of armed force that fit into the first sentence and constitute an act of aggression.[26]

---

[19] Rome Statute, *supra* note 16, art. 8*bis*, ¶ 2(a).
[20] *Id.* ¶ 2(b).
[21] *Id.* ¶ 2(c).
[22] *Id.* ¶ 2(g).
[23] *Id.* ¶ 2(f).
[24] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. Rep. 226, ¶ 39 (July 8) [hereinafter Legality of the Threat or Use of Nuclear Weapons].
[25] Rome Statute, *supra* note 16, art. 22. *See also* Noah Weisbord, *Conceptualizing Aggression*, 20 DUKE J. COMPAR. & INT'L L. 1, 40 (2009).
[26] Matthew Gillett, *The Anatomy of an International Crime: Aggression at the International Criminal Court*, 13 INT'L CRIM. L. REV. 829, 844 (2013) (citing ICC, *Report of the Special Working Group on the Crime of Aggression*, at ¶ 34, ICC-ASP/6/20/Add.1/ Annex II)).

5. The Council also agreed that cyber operations could fit under the enumerated examples listed in Article 8*bis*. Those most easily identifiable were: (b) bombardment, (c) blockade of ports, (d) an attack on the armed forces of another state, (f) allowing one's territory to be used by another state to commit aggression, and (g) the sending of "armed bands."

Threshold Clause

A use of armed force must reach the threshold of a manifest violation of Article 2(4) of the UN Charter as justified by its character, gravity, and scale to amount to a crime of aggression under Article 8*bis*.

6. Cyber operations vary widely in their character, gravity, and scale. Some are a nuisance, while others cause as much destruction as a kinetic attack. The Council of Advisors considered how serious and far-reaching the consequences of a cyber operation must be to qualify as an act of aggression under the threshold established in Article 8*bis* of the Rome Statute. This inquiry called for the Council of Advisers to discuss the meaning of the phrases "manifest violation" of the UN Charter and sufficient "character, gravity and scale" in Article 8*bis*, and what exactly those terms entail in the context of cyber operations.

7. The meaning and scope of "manifest" in Article 8*bis* is addressed in the Elements of Crimes and Understandings attached to the text of the Kampala amendments.[27] The relevant introduction to the Elements and Understandings reads as follows:

> Introduction to the Elements 3: "the term 'manifest' is an objective qualification."[28]
>
> Understanding 6: "It is understood that aggression is the most serious and dangerous form of the illegal use of force; and that a determination whether an act of aggression has been committed requires consideration of all the circumstances of each particular case, including the gravity of the acts concerned and their consequences, in accordance with

[27] ROGER S. CLARK, *Negotiations on the Rome Statute, 1995–98*, *in* THE CRIME OF AGGRESSION: A COMMENTARY 244–270 (Claus Kreß & Stefan Barriga eds., 2016).
[28] Kampala Amendments, *supra* note 15, Annex II.

> the Charter of the United Nations."[29]
>
> Understanding 7: "It is understood that in establishing whether an act of aggression constitutes a manifest violation of the Charter of the United Nations, the three components of character, gravity and scale must be sufficient to justify a 'manifest' determination. No one component can be significant enough to satisfy the manifest standard by itself."[30]

8. This has been read to mean that "a breach of the prohibition of the use of force will only amount to aggression where it is a grave violation with serious consequences."[31] In other words, it ensures that only serious and unambiguously illegal instances of a use of force by a State can give rise to individual criminal responsibility of a leader of that State under the Statute. It has also been suggested that the "manifest violation" element requires an inquiry into the magnitude of the unlawful use of force.[32] It is clear by the use of the term "manifest"—meaning clear, apparent, or evident—that the act must be more than an illegal use of force.[33]

9. The Council of Advisers agreed that exactly what a "manifest" violation of the UN Charter means in the context of cyber operations has not been established. Neither State practice nor jurisprudence delineates a threshold for cyber operations to run afoul of Article 2(4) of the UN Charter in a "manifest" manner. Further developments in both technology and State practice will help to solidify this issue.

10. Not only does a use of armed force need to be a "manifest" violation of Article 2(4) of the UN Charter, it must be manifest "by its character, gravity, and scale."[34] Members of the Council of Advisers reached different conclusions about what this means in a general context, even when setting aside the

---

[29] *Id.* Annex III.

[30] *Id.*

[31] Dapo Akande, *What Exactly Was Agreed in Kampala on the Crime of Aggression?*, EJIL: TALK! – BLOG OF THE EUROPEAN JOURNAL OF INTERNATIONAL LAW (June 21, 2010), https://www.ejiltalk.org/what-exactly-was-agreed-in-kampala-on-the-crime-of-aggression/.

[32] Keith A. Petty, *Criminalizing Force: Resolving the Threshold Question for the Crime of Aggression in the Context of Modern Conflict*, 33 SEATTLE U. L. REV. 105, 116 (2009).

[33] *See* International Criminal Court, Assembly of States Parties, Fifth Session, ICC-ASP/5/SWGCA/1, *Report of the Special Working Group on the Crime of Aggression*, ¶ 8 (Nov. 29, 2006).

[34] Rome Statute, *supra* note 16, art. 8*bis*, ¶ 1. *See also* Draft Policy on Cultural Heritage, INTERNATIONAL CRIMINAL COURT (2021), https://www.icc-cpi.int/itemsDocuments/2021-03-22-otp-draft-policy-cultural-heritage-eng.pdf (last visited Jul 2, 2021), ¶¶ 89-92.

specific context of a cyber operation. It is agreed that a manifest violation cannot be proven with only one of the three criteria of character, gravity, and scale, but members of the Council generally agreed that two of the three are sufficient to determine a manifest violation. Some members of the Council expressed the view that the character element had to be fulfilled in any case while the elements of gravity and scale could be applied in the form of a sliding scale.

11. The threshold of "character" is meant to refer to cases of genuine legal controversy.[35]

12. "Gravity" connotes the extent of damage that resulted to life, limb or property. The ICC case law has indicated in its interpretation of other crimes 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.[36]

13. The word "scale" refers to the magnitude of the attack. This could encapsulate numerous considerations ranging from resources employed, to the level of planning and coordination undertaken, or extent of the consequences of the attack.

14. The Tallinn Manual proposes an eight-factor test to assess cyber operations in the context of use of force and armed attacks.[37] The Council of Advisers highlighted that this is one possible starting point for the question of threshold for the purposes of Article 8*bis*, but noted that it cannot be dispositive, as use of force and armed attack are distinct from a "manifest" violation of Article 2(4) by its "character, gravity and scale."

---

[35] Kevin L. Miller, *The Kampala Compromise and Cyberattacks: Can There Be an International Crime of Cyber-Aggression?*, 23 S. CAL. INTERDISC. L. J. 217 (2014). One member of the Council proposed that if the motive behind a cyber operation is particularly malicious, it could compensate for a somewhat lesser intensity of the unlawful use of force in the analysis of the threshold requirement in Article 8*bis*. In other words, when weighing character, gravity and scale together, the particularly malicious character of an attack could tip the scale toward the finding that an act of aggression has been committed. Others thought this inconsistent with the language of Article 8*bis*.

[36] Prosecutor v. Abu Garda, ICC-02/05-02/09, Decision on the Confirmation of Charges, ¶¶ 31–32 (Feb. 8, 2010); Situation in the Republic of Kenya, ICC-01/09-19-Corr, Decision Pursuant to Article 15 of the Rome Statute on the Authorization of an Investigation into the Situation in the Republic of Kenya, ¶ 62 (Mar. 31, 2010).

[37] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 334–36, r. 69 (Michael N. Schmitt ed., 2d ed. 2017).

15. Members of the Council of Advisers did not fully agree with regard to what types of cyber operations involving a use of force within the meaning of Article 2(4) could fulfill the threshold requirement. A few took the position that only cyber operations resulting in loss of, or injury to, human life would reach the level of a "manifest" violation of the prohibition of the use of force. Some accepted that cyber operations with large-scale physical destruction could also reach the level of a manifest violation. Others suggested loss of functionality or incapacitation, without physical destruction, could be considered.

16. There was general agreement among the members of the Council that cyber operations with purely economic impacts would not reach the level of a "manifest" violation of Article 2(4) of the UN Charter. Similarly, election interference and attacks on financial infrastructure, depending on their consequences, were generally considered by the Council not to meet Article 8bis' threshold clause because such cyber operations, although contrary to international law (e.g. the principle against non-intervention), do not fit into the aggression framework. Some members of the Council, however, raised the need for further careful consideration of these questions.

17. The Council of Advisers agreed that it would not be wise to lower the threshold of what constitutes a violation of Article 2(4) of the UN Charter. The Council of Advisers noted in particular that the UN Charter's Article 51 doctrine of individual and collective self-defense is already interpreted too broadly by some (the United States, for example, currently considers the Article 2(4) and Article 51 thresholds to be the same), given that lowering the "use of force" threshold could open the door to retaliatory actions under Article 51.[38] Some Council members noted that States have other tools in their toolbox, in particular diplomatic and economic tools, to address such situations. Moreover, actions that do not violate Article 2(4) may be unlawful violations of the principle of non-intervention.

---

[38] Noah Weisbord, The Crime of Aggression: The Quest For Justice in an Age of Drones, Cyberattacks, Insurgents, and Autocrats 137–38 (Eric D. Weitz ed., 2019).

18. There was considerable disagreement among the Council of Advisers with regard to the question of accumulation of events. This proposition suggests that a series of attacks, none of which would individually amount to an armed attack, could nonetheless collectively constitute an armed attack. The ICJ has not explicitly endorsed this argument, but some have argued that it has implicitly done so: it has on multiple occasions ruled that a series of individual attacks did not, on the facts, amount to an armed attack, while not rejecting this legal theory wholesale.[39] This doctrine has not yet been applied to the crime of aggression in any context, cyber or kinetic; thus, the Council of Advisers left this question open for further consideration.[40]

19. The Council of Advisers left other issues unsettled, in particular with regard to the analysis of damage to intellectual versus physical property, state property versus private property, and damage to critical infrastructure that is highly disruptive but does not involve damage to life, limb, or property. The Council of Advisers cautioned that this ground must be trodden upon very carefully since it can result in dilution of the threshold for use of force more broadly. As noted above, such a dilution would have negative implications for the triggering of self-defense, countermeasures and other related measures.

---

[39] *See* Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶ 64 (Nov. 6); Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, ¶ 147 (Dec. 19); Steven R. Ratner, *Self-Defense Against Terrorists: The Meaning of Armed Attack*, *in* COUNTER-TERRORISM STRATEGIES IN A FRAGMENTED LEGAL ORDER: MEETING THE CHALLENGES 334 (Larissa van den Herik & Nico Schrijver eds., 2013).

[40] Some on the Council of Advisers considered that cyber operations close in time on the same target might potentially reach the level of a manifest violation of the UN Charter for the purposes of Article 8*bis*. This aligns with the French position that cyber operations that do not in isolation reach the threshold of aggression could qualify as an act of aggression if the accumulation of their effects reaches a sufficient level of severity, or if the attacks are carried out concurrently with kinetic attacks that amount to aggression. *See also* MINISTÈRE DES ARMÉES, DROIT INTERNATIONAL APPLIQUÉ AUX OPÉRATIONS DANS LE CYBERSPACE 8–9, § 1.2.1 (2019), https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+international+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf. However, other Council members were more hesitant about accumulation, both in general and with respect to cyber operations. Regarding the disagreement around when a series of events could cumulatively constitute an armed attack, *see also* Stefan Soesanto, WHEN DOES A 'CYBER ATTACK' DEMAND RETALIATION? NATO BROADENS ITS VIEW DEFENSE ONE (2021), https://www.defenseone.com/ideas/2021/06/when-does-cyber-attack-demand-retaliation-nato-broadens-its-view/175028/ (last visited July 7, 2021).

Leadership Clause

A leader who prepares, plans, initiates, or executes a cyber operation can be found to have violated Article 8*bis* if the other criteria of the crime have been met. A leader for the purposes of individual criminal responsibility for a crime of aggression committed through cyber means could mean high-level leaders of the political, military or intelligence branches of government (including those overseeing cyber command structures), or individuals without a formal post but who are "in a position effectively to exercise control over or to direct the political or military action of a State."

20. The Rome Statute of the ICC designates individual criminal responsibility as the main mode of attributing responsibility under Article 25. The applicability of this Article to the crime of aggression is limited "only to persons in a position effectively to exercise control over or to direct the political or military action of a State."[41] This is the "leadership clause" under which superiors may be held responsible for acts whose execution they plan, prepare, initiate, or execute. Members of the Council made the distinction between having "effective control" (as seen in the command responsibility language in Article 28) and being "in a position effectively to exercise" control (as seen in Article 8*bis*). Regardless, the leader not only needs to be in a position to exercise control but needs to be involved in the preparation, planning, initiation or execution of an act of aggression to be held responsible.[42] The Council cautioned that this language should not be conflated with the effective control test under the doctrine of state responsibility, as it could raise the threshold higher than it ought to be.

21. Aggression under Article 8*bis* is a purely leadership offence committed by persons capable of controlling political or military decisions,[43] and any individual to whom the conduct is attributed must meet the threshold

---

[41] Rome Statute, *supra* note 16, art. 8*bis* in conjunction with art. 25(3)*bis*. *See also* Hannah Lea Pfeiffer, THE CRIME OF AGGRESSION AND THE PARTICIPATION MODEL OF THE ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT (Claus Kreß ed., 2017).

[42] Volker Nerlich, *The Crime of Aggression and Modes of Liability – Is There Room Only for Principals?*, 58 HARV. INT'L L. J. 44 (2017); *see* Weisbord *supra* note 38 at 145.

[43] Surendran Koran, *The International Criminal Court and Crimes of Aggression: Beyond the Kampala Convention*, 34 HOUSTON J. INT'L L. 231, 255 (2012).

discussed above. Nonetheless, in cyberwarfare, due to the precise tactical and strategic decisions necessary to carry out an attack, some members of the Council noted it is possible to reach relatively far down the chain of command. Other Council members noted that the nature of cyberwarfare means that it can be harder to attribute leadership and decision-making in these circumstances than in kinetic warfare.[44]

22. The Council of Advisers agreed that a leader for the purposes of individual criminal responsibility for a crime of aggression committed through cyber operations could mean high-level leaders of the political, military or intelligence branches of government (including those overseeing cyber command structures), and potentially non-state actors "in a position effectively to exercise control over or to direct the political or military action of a State."

23. The Council agreed that the situation of a leader who gives "blank check" delegation would be treated the same way in cyber and kinetic attacks. Members of the Council were divided on whether broad delegation would be prosecutable, or whether it might depend on how involved a particular administration was in planning preparation, initiation or execution of a cyber operation.

Acts of Aggression by Non-State Actors

It may prove difficult for non-state actors to be successfully prosecuted by the ICC for their cyber acts of aggression due to the limitations in Article 8*bis*.

24. Article 8*bis* defines an act of aggression as "the use of armed force *by a State*,"[45] which by a plain reading would thereby exclude uses of such force by non-state actors, even if the grave effects of the latter are equivalent to attacks by states themselves.

25. The Council of Advisers acknowledged the significant proliferation of non-state actors in cyberwarfare largely because of its low entry and cost barriers.

---

[44] Still, some serious cyber operations to date have been attributable, with a great deal of confidence, to a state or states, and even to specific leaders. *See* DAVID E. SANGER, THE PERFECT WEAPON: WAR, SABOTAGE, AND FEAR IN THE CYBER AGE (2019).

[45] Rome Statute, *supra* note 16, art. 8*bis*, ¶ 2 (emphasis added).

26. In the discussions, some members of the Council raised the international law on attribution as the mechanism through which states can be held accountable for actions of non-state actors, while acknowledging this report is focused primarily on individual criminal responsibility. However, for state responsibility to arise, the narrow attribution criteria need to be fulfilled.[46] For the acts of a non-state actor to be attributed to a state, the non-state actor that commits an attack must (1) be an organ or agent of a state,[47] or (2) perform governmental functions,[48] or (3) act under the instructions, direction or effective control of a state.[49] These are the criteria employed by the ICJ as well.[50] Two other potential attribution standards discussed were the "overall control" test from the ICTY's decision in *Tadić*, and the "sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries . . . or its substantial involvement therein" from Article 8*bis* (2)(g) of the Rome Statute, based on the General Assembly's 1974 Definition of Aggression.[51]

27. Other Council members raised the possibility of individual criminal responsibility under Article 25 of the Rome Statute. As noted in the previous section, the applicability of this Article to the crime of aggression is limited "only to persons in a position effectively to exercise control over or to direct the political or military action of a State."[52] Since the provisions of this article are silent as to whether they apply to both state and non-state actors, the silence could be interpreted to mean two things: (1) that non-state actors may be prosecuted under this clause if they were the leaders of a cyber operation and in a position to exercise political or military action of a State, or (2) that a State's leader who engages non-

---

[46] *See* International Law Commission, *Responsibility of States for Internationally Wrongful Acts*, U.N. Doc. A/56/10 Supplement No. 10 (2001) (*see* G.A. Res 56/83 (Dec. 12, 2001)).

[47] *Id.* ch. II, art. 4.

[48] *Id.* arts. 5–6.

[49] *Id.* art. 8.

[50] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14 [hereinafter *Nicaragua* Case], at ¶ 163. *See also* Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Rep. 43, ¶¶ 400-407 (Feb. 26, 2007).

[51] For a recent discussion of those standards, *see* Claus Kreß, *AGGRESSION*, *in* THE OXFORD HANDBOOK OF THE INTERNATIONAL LAW OF GLOBAL SECURITY 232–253 (Robin Geiß & Nils Melzer eds., 2021).

[52] Rome Statute, *supra* note 16, art. 25, ¶ 3*bis*.

State actors to conduct cyber operations could potentially be covered if all the other required elements of the crime were satisfied (such as attribution of the acts of the non-State actors to the State whose leader engaged them).

28. The Council of Advisers acknowledged that establishing a connection between State leadership and non-State actors may be difficult for the purposes of Article 8*bis* criminal responsibility in the context of cyber-operations, but left the question open for further consideration.[53]

SECTION III

The following section reflects the Council of Advisers' discussion on the jurisdiction of the ICC under Articles 15*bis* and 15*ter* of the Rome Statute.[54]

Article 15*bis* Jurisdiction of the Court for the Crime of Aggression by State Referral or the *Proprio Motu* Power

29. Article 15*bis* seems to provide the Court with jurisdiction over the crime of aggression in a conflict between any two State Parties, provided that at least one of them has accepted the Kampala amendments and the aggressor State has not opted out of the Court's jurisdiction. The decision adopted by the Assembly of States Parties activating the Court's jurisdiction over the crime of aggression can be read as not fully

---

[53] One member of the Council recalled that it was the submission of Benjamin Ferencz, for the Prosecution at Nuremberg, that non-state actors might be responsible for aggression. Specifically, the Prosecution in the *Krupp Case* accused defendants who "held high positions in the political, financial, industrial, and economic life of Germany and committed crimes against peace in that they were principals in, accessories to, ordered, abetted, took a consenting part in, were connected with plans and enterprises involving, and were members of organizations and groups, including Krupp, connected with the commission of crimes against peace." U.S. v. Krupp, 9 TRIALS OF WAR CRIMINALS BEFORE THE NUERNBERG MILITARY TRIBUNALS UNDER CONTROL COUNCIL LAW NO. 10, at 10 (1950) (noting Benjamin Ferencz as Special Prosecution Counsel).

[54] *See* NIELS BLOKKER & STEFAN BARRIGA, *Conditions for the Exercise of Jurisdiction Based on Security Council Referrals*, *in* THE CRIME OF AGGRESSION: A COMMENTARY 646–651 (Claus Kreß & Stefan Barriga eds., 2016). *Also see* STEFAN BARRIGA & NIELS BLOKKER, *Conditions for the Exercise of Jurisdiction Based on State Referrals and Proprio Motu Investigations*, *in* THE CRIME OF AGGRESSION: A COMMENTARY 652–674 (Claus Kreß & Stefan Barriga eds., 2016).

consistent with the language of Article 15*bis*. The same decision recalls that the interpretation of the relevant legal provisions is left to the ICC judges by recalling the independence of the Court.[55]

30. After a brief discussion, the Council of Advisers agreed that how Article 15*bis* ultimately applies, both generally and specifically in the context of cyber acts of aggression, requires judicial interpretation. Some members of the Council recalled that the language of the ASP resolution activating the Court's jurisdiction over the crime of aggression reaffirmed "paragraph 1 of article 40 and paragraph 1 of article 119 of the Rome Statute in relation to the judicial independence of the judges of the Court."[56] This reaffirmation was suggested to mean that the ICC's judges alone can provide the necessary clarity on how the jurisdictional provisions in Article 15*bis* apply.

31. The Council acknowledged that as technology continues to advance and cyber operations become an increasingly important tool for States, the ICC will likely have occasion to provide the necessary clarity on the application of Rome Statute Article 15*bis* on the jurisdiction of the Court over the crime of aggression in instances of State referral or consideration of the possibility of *proprio motu* investigations.

32. The Council of Advisers also discussed jurisdiction in the context of cyber acts of aggression where several States have been involved in a cyber operation, with or without their knowledge.[57] The Council considered the example of NotPetya, a cyber operation which was meant to target Ukraine but had far-reaching consequences on private industry in other countries. Any unanticipated collateral damage, though possibly reckless, would not be considered a crime of aggression because of the lack of sufficient *mens rea*.[58]

---

[55] Resolution ICC-ASP/16/Res.5, *supra* note 17, at ¶ 3.

[56] *Id.* For one interpretation, *see* Jennifer Trahan, *From Kampala to New York—The Final Negotiations to Activate the Jurisdiction of the International Criminal Court over the Crime of Aggression*, 18 INT'L CRIM. L. REV. 197 (2018).

[57] *See generally* Alexandra Perloff-Giles, *Transnational Cyber Offenses: Overcoming Jurisdictional Challenges*, 43 YALE J. INT'L L. 191 (2018).

[58] For example, the NotPetya creators likely only intended to damage Ukrainian targets, so they would not have had the *mens rea* needed to be guilty of the crime of aggression in connection with damage to non-Ukrainian computers systems. *See* Andy Greenberg, *The Untold Story of NotPetya, The Most Devastating Cyberattack in History,* WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (describing the NotPetya malware and its devastating impact). *See also* Noah Weisbord, *The*

In addition, jurisdiction would likely not be created where one country executes a cyber operation routed through servers in several different countries; only the country where the attack originated (aggressor State) and ended (victim State) is relevant for consideration of jurisdiction.

Article 15*ter* Jurisdiction of the ICC for the Crime of Aggression by United Nations Security Council Referral

33. The Council of Advisers agreed that the ICC is able to investigate and prosecute crimes of aggression following a UN Security Council referral without any further aggression-specific conditions. This means that there is no requirement for the involved States to give any type of consent to the investigation because the Court's jurisdiction under Article 15*ter* of the Rome Statute is a result of the Security Council referral under Chapter VII of the UN Charter.

34. The Council also noted that the Security Council is not required to make any determination that there was an act of aggression in order to make a referral to the ICC. The Security Council is, of course, not precluded from making such a determination, but even if it did, Article 15*ter*(4) states that "[a] determination of an act of aggression by an organ outside the Court shall be without prejudice to the Court's own findings under this Statute."[59]

35. The ICC, therefore, has the widest jurisdiction with respect to the crime of aggression when a situation is referred to it by the UN Security Council, as this would lift the State referral or *proprio motu* limitations related to the Court's jurisdictional regime. The Council of Advisers agreed, however, that current political difficulties of galvanizing the Security Council toward accountability make such a referral difficult to attain.

Mens Rea of The Crime of Aggression, 12 WASH. U. GLOB. STUD. L. REV. 487, 497 (2013), https://openscholarship.wustl.edu/law_globalstudies/vol12/iss3/10.

[59] For additional discussion of the role of the Security Council in making referrals related to the crime of aggression, *see, e.g.*, Jennifer Trahan, *Revisiting the Role of the Security Council Regarding the International Criminal Court's Crime of Aggression*, 17 J. INT'L CRIM. JUST. 471 (2019).

SECTION IV: CONCLUSION

36. Based on their discussion, the Council of Advisers agreed that a cyber operation would qualify under the enumerated list of acts of aggression in Article 8*bis* for two reasons: (1) the list is illustrative, not exhaustive, and (2) cyber operations could qualify under a number of the enumerated examples listed in Article 8*bis*. The Council also agreed that—because Article 8bis requires the attack qualifying as an act of aggression to be a "manifest violation of the Charter of the United Nations"—a cyber operation without loss of, or injury to, human life, or large-scale physical destruction (e.g., military systems or critical structure) may only rarely lead to prosecution for the crime of aggression under the Rome Statute. With respect to the Court's complex jurisdiction regime over the crime of aggression, the Council acknowledged that how Article 15*bis* applies to cyber acts of aggression will depend on how ICC judges square the Kampala amendments on the crime of aggression with the Assembly of States Parties' activating decision.[60]

37. As technology continues to advance on and off the battlefield and war-making organizations continue to evolve, it has become clear that cyber technologies will play a role in international criminal acts, including the commission of aggression. Though the Council of Advisers attempted, in its discussion of various present and future scenarios, to anticipate the ways that cyber conduct will be interpreted by the ICC in the context of the crime of aggression, there remained open questions, such as: How directly must loss of life be connected to a cyber operation to be considered a result of the attack? Might a lower scale attack lead to a crime of aggression prosecution if it compromised critical infrastructure or military systems? Could a cyber operation that caused grave impact on an economic system lead to a crime of aggression prosecution? Could a series of smaller scale but related attacks be accumulated to lead to a crime of aggression prosecution? Are there scenarios where critical data deletion (such as crucial medical data) could lead to a crime of aggression prosecution? The Advisers considered the application of the crime of aggression in a future when people's online property and identities become increasingly central to their security and well-being. In the context of the

[60] Resolution ICC-ASP/16/Res.5, *supra* note 17.

threshold clause discussed above, could character be elevated vis-à-vis gravity and scale to lead to a crime of aggression prosecution? How should "sending of armed bands" be interpreted in the context of cyber operations? Moreover, the Council also left open the question of what the primary protected values in deterring crimes of aggression are, namely are they political independence and sovereignty or do they also include ensuring peace, civilian protection and human rights?[61]

38. The Council agreed that individual criminal responsibility can follow cyber operations. It concluded that further discussion of potential aggression scenarios would be constructive, providing greater clarity about the scope of criminal responsibility to leaders, political advisors, the judiciary, legislatures, and the media.

[61] For a discussion of this question, *see generally* Frédéric Mégret, *What is the Specific Evil of Aggression?*, THE CRIME OF AGGRESSION, *supra* note 1, at 1398.

PART II

The Application of Article 8 (War Crimes) of the Rome Statute to Cyberwarfare

PART II: THE APPLICATION OF ARTICLE 8 (WAR CRIMES) OF THE ROME STATUTE TO CYBERWARFARE

SECTION I

War Crimes in the International Criminal Court: General Overview

Article 8 of the Rome Statute gives the ICC jurisdiction with respect to war crimes committed in the context of both International Armed Conflict (IAC)[62] and Non-International Armed Conflict (NIAC).[63] The Rome Statute provisions on war crimes are unique in that they codify decades of law and practice, but also add a comprehensive section on war crimes during a NIAC and add new crimes, such as attacks on peacekeepers.[64]

Article 8(1) sets out a specific threshold for war crimes, namely that: "[t]he Court shall have jurisdiction in respect of war crimes in particular when committed as part of a plan or policy or as part of a large-scale commission of such crimes."[65] The ICC has clarified through its previous judgments that the two requirements serve as alternatives and that one need not provide evidence of both to reach the threshold of a war crime.[66] Furthermore, the ICC has stated that the words, "in particular" in Article 8(1) qualify the threshold requirements and that the threshold should serve as a guideline for the Court.[67] In other words, a large-scale commission or the existence of a policy or plan is not imperative for ICC

---

[62] Rome Statute, *supra* note 16, art. 8, ¶ 2(a)–(b).

[63] *Id.* ¶ 2(c)–(f).

[64] *See* WILLIAM A. SCHABAS, THE INTERNATIONAL CRIMINAL COURT: A COMMENTARY ON THE ROME STATUTE 221 (2d. ed. 2016).

[65] Rome Statute, *supra* note 16, art. 8, ¶ 1.

[66] Situation in the Democratic Republic of the Congo, ICC-01/04, 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," ¶ 70 (July 13, 2006). *See also* SCHABAS, *supra* note 64, at 226.

[67] Situation in the Democratic Republic of the Congo, ICC-01/04, 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," ¶ 70 (July 13, 2006). *See also* SCHABAS, *supra* note 64, at 226.

jurisdiction over war crimes; one single act might also qualify as a war crime under the Rome Statute.[68]

Irrespective of whether an act is kinetic or in cyberspace, Article 8 of the Rome Statute can only be applied if certain conditions exist to trigger the application of International Humanitarian Law (IHL).[69] First, as a matter of customary international law and supported in the Rome Statute and Elements of Crimes,[70] war crimes must take place in the context of armed conflict, either international or non-international.[71] Practically applied, there must exist an ongoing armed conflict, or the act itself must rise to such a level so as to trigger IHL.[72] Importantly, the Rome Statute does not provide a definition for international or non-international armed conflict;[73] provisions within Article 8 pertaining to international and non-international armed conflict reflect provisions in IHL.[74] Second, the armed conflict will, in most cases, have a territorial link.[75] Third, there must be a nexus between the armed conflict and the subject-matter of the investigation or prosecution at the Court,[76] such that it occurred "in the context of and was associated with international [or non-international] armed conflict."[77]

---

[68] *See* SCHABAS, *supra* note 64, at 226.

[69] *See* Kai Ambos, *International Criminal Responsibility in Cyberspace*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 118, 121 (Nicholas Tsagourias & Russell Buchan eds., 2015).

[70] *See* SCHABAS, *supra* note 64, at 225; JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW: VOLUME 1: RULES, 568–603 (2005); Rome Statute, *supra* note 11, art. 8 ¶ 2 (describing war crimes as certain breaches of the Geneva Conventions, which only apply during armed conflict, or other violations of laws and customs during either international or non-international armed conflicts); Preparatory Commission for the International Criminal Court, *Report of the Preparatory Commission for the International Criminal Court, Addendum*, add. Part II Finalized draft text of the Elements of Crimes, U.N. Doc. PCNIC/2000/1/Add.2, at 18 (2000) [hereinafter Elements of Crimes] (describing a requirement that perpetrators of war crimes be aware "of the factual circumstances that established the existence of an armed conflict").

[71] *See* SCHABAS, *supra* note 64, at 228.

[72] *See* Ambos, *supra* note 69, at 121–22; HENCKAERTS & DOSWALD-BECK, *supra* note 70, at 568–603.

[73] *See* SCHABAS, *supra* note 64, at 228–29.

[74] *See id.*

[75] *See* Ambos, *supra* note 69, at 126.

[76] Tadić Jurisdictional Decision (n 20) [70]; Prosecutor v. Aleksovski (Judgment) ICTY95-14/1-T (25 June 1999) [45]; Prosecutor v. Musovic *et. al.* (Judgment) ICTY-96-21-T (16 November 1998) [193]; see also Werle and Jessberger (Principles) (n 13) mn. 1109 *et seq.* (with further references).

[77] Elements of Crimes, *supra* note 70. This element is listed for all of the enumerated crimes

Fourth, the perpetrator must have knowledge of the existence of the armed conflict,[78] although they need not perform any kind of legal evaluation, including as to its character.[79] The accused must merely be aware of "the factual circumstances that established the existence of an armed conflict."[80]

SECTION II

1. The Council of Advisers unanimously agreed that cyber operations may qualify as war crimes if they are undertaken during either an IAC or a NIAC, as defined by IHL, and if the cyber operation falls under any of the acts listed in Article 8(2).[81] The use of cyber operations during armed conflicts—just like the use of any other weapon, means and methods of warfare in an armed conflict, whether new[82] or old—is subject to the rules and principles of IHL.[83] As such, civilians and members of armed forces

---

in Article 8(2).

[78] *See* SCHABAS, *supra* note 64, at 237.

[79] *See* Elements of Crimes, *supra* note 70, at 18.

[80] *Id.*

[81] Each of the acts listed in Article 8(2) constitutes a serious breach of IHL and Common Article 2 of the Geneva Conventions stipulates that application of IHL is predicated on the existence of an armed conflict. *See* Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 2, Aug. 12, 1949, 75 U.N.T.S. 31 [hereinafter Geneva Convention I]; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea art. 2, Aug. 12, 1949, 75 U.N.T.S. 85 [hereinafter Geneva Convention II]; Geneva Convention relative to the Treatment of Prisoners of War art. 2, Aug. 12, 1949, 75 U.N.T.S. 135 [hereinafter Geneva Convention III]; Geneva Convention relative to the Protection of Civilian Persons in Time of War art. 2, Aug. 12, 1949, 75 U.N.T.S. 267 [hereinafter Geneva Convention IV]; *see also* Prosecutor v. Tadić, Case No. IT-94-1-I, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

[82] International security experts began considering the possibility of cyberwarfare in the mid-1990s. *See* Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis*, 25 STAN. L. & POL'Y REV. 269, 269 (2014); *see also* Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts art. 36, June 8, 1977 [hereinafter Additional Protocol I].

[83] Legality of the Threat or Use of Nuclear Weapons, *supra* note 24, ¶ 86 (July 8) (noting that merely because nuclear weapons were invented after most of the principles of humanitarian law applicable to armed conflict were established does not mean IHL does not apply and opining that a contrary conclusion "would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of

involved in cyber operations in the context of an armed conflict may be held criminally responsible for violations of IHL under Article 8 of the Rome Statute, despite the relatively recent appearance of cyber operations in the world of armed conflict.[84] That said, the unique nature of cyber operations raises a number of issues related to the application of Article 8, each of which is taken up in turn below.

Existence of an Armed Conflict

Where an ongoing armed conflict exists, violations of international humanitarian law may constitute a war crime under Article 8 of the Rome Statute. Whether a cyber operation on its own could trigger an international or non-international armed conflict is not a settled issue.

2. As stated in the introduction to this chapter, criminal conduct under Article 8 depends on the existence of an armed conflict—individuals who engage in criminal or other malicious cyber activities entirely unrelated to armed conflict are beyond the scope of Article 8.[85] Therefore, the preliminary question when analyzing whether a cyber operation constitutes an Article 8 War Crime is whether the operation or attack was undertaken in the context of an armed conflict, including by initiating such a conflict. Although there is no definition of armed conflict in the Rome Statute,[86] the generally accepted definition from the *Tadić* decision, is that "an armed conflict exists whenever there is a resort to armed force

---

the past, those of the present and those of the future."). *See also, e.g.*, Terry D. Gill, *International humanitarian law Applied to Cyber-Warfare: Precautions, Proportionality and the Notion of 'Attack' Under the Humanitarian Law of Armed Conflict, in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 366, 367 (Nicholas Tsagourias & Russell Buchan eds., 2015); International Committee of the Red Cross, *International Humanitarian Law and the challenges of contemporary armed conflicts* 36-37 (2011); International Committee of the Red Cross, *International humanitarian law and the challenges of contemporary armed conflicts* 40 (2015); International Committee of the Red Cross, *International Humanitarian Law and Cyber Operations during Armed Conflicts* 2 (2019).

[84] *See* TALLINN MANUAL 2.0, *supra* note 37, at 392.

[85] *See id.* at 376, 392.

[86] Prosecutor v. Bemba, 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, ¶ 217 (June 15, 2009) [hereinafter *Bemba* Decision].

between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State."[87] The Council of Advisers agreed that where a cyber operation is undertaken during an ongoing armed conflict, the threshold for armed conflict has already been met, so any qualifying violation of IHL that occurs as a result of a cyber operation could constitute a war crime.[88] But where a cyber operation is carried out independently of an ongoing conflict, the question becomes whether cyber operations alone can begin an international or non-international armed conflict and thus fall within the jurisdiction of the ICC.

3. In considering this question, before looking to the specific requirements and limitations with respect to IAC and NIAC, the Council of Advisers considered more generally that regardless of whether the relevant conduct occurred in cyberspace or not, the existence of an armed conflict will depend on "whether armed force has been employed and whether this can be attributed to one party to the conflict."[89] In accordance with accepted doctrine,[90] the Council of Advisers assessed the question of whether or not a cyber operation could constitute armed force based on the "effects" method, rather than the "means" method.[91] Indeed, it has

---

[87] Prosecutor v. Tadić, Case No. IT-94-1-l, Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l. Crim. Trib. for the Former Yugoslavia Oct. 2, 1995) [hereinafter *Tadić* Decision on the Defense Motion]; *see also* Prosecutor v. Lubanga, ICC-01/04-01/06, Judgment pursuant to Article 74 of the Statute, ¶ 533 (Mar. 14, 2012) [hereinafter *Lubanga* Judgment] (endorsing the definition of armed conflict articulated in *Tadić* Decision on the Defense Motion).

[88] *See* Ambos, *supra* note 69, at 122. In order to constitute a war crime under Article 8, in addition to taking place in the context of an armed conflict, the remaining conditions outlined in the introduction to this chapter must be met, and the conduct must satisfy the definition of one of the crimes listed in Article 8(2)(a), (b), (c), or (e). It is important to note that, to be prosecuted at the ICC, such an act must also be charged as part of a case that reaches the ICC gravity threshold for admissibility per Rome Statute art. 17(1)(d).

[89] Ambos, *supra* note 69, at 122.

[90] *See, e.g.,* Karine Bannelier-Christakis, *Is the Principle of Distinction Still Relevant in Cyberwarfare?, in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 343, 348-49 (Nicholas Tsagourias & Russell Buchan eds., 2015). *See also* Ambos, *supra* note 69, at 123; Anne-Laure Chaumette, *International Criminal Responsibility of Individuals in Case of Cyberattacks*, 18 INT'L CRIM. LAW REV. 1, 11 (2018); Nils Melzer, *Cyber Operations and* Jus in Bello, 4 DISARMAMENT FORUM 1, 7 (2011); Michael N. Schmitt, *Cyber Operations and the* Jus in Bello*: Key Issues*, 87 INT'L L. STUD. 89, 95 (2011).

[91] *See* Ambos, *supra* note 69, at 123–24; Cordula Droege, *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, 94 INT'L REV. RED CROSS 533, 546 (2012). This distinction seeks to clarify whether armed force is found to

been argued that a computer network attack that causes damage comparable to a traditional kinetic use of armed force could meet the necessary threshold for armed conflict.[92] The Council of Advisers was divided on this question, to be discussed further below.[93]

4. Regardless of whether an attack is launched by a State, an organized or non-organized group or an individual, the Council of Advisers recognized that attribution of the attack to a given actor may present serious difficulties, due to the nature of cyber operations. For example, given the difficulty of tracing cyber operations, it is possible for one State to pose as another (so called "false flag" operations).[94] The Council of Advisers discussed recent reports that certain groups of hackers from one State were able to launch hostile cyber operations while disguised as hackers acting on behalf of another State. Members of the Council of Advisers added that a further challenge with attribution is the lack of information sharing among government bodies. The Council of Advisers noted, however, that ability to attribute cyber operations is advancing.

Whether Cyber Operations Can Trigger International Armed Conflict

A State that has overall control of a non-State armed group and directs that group to launch a cyber operation that causes substantial physical damage in the territory of another state could constitute an international armed conflict, and therefore, fall under the jurisdiction of Rome Statute Article 8. The use-of-force threshold that triggers

---

have been used by virtue of the effects of the actions or by virtue of the means used to cause such an effect.

[92] *See* International Committee of the Red Cross, COMMENTARY ON THE THIRD GENEVA CONVENTION ¶ 288 (2020), https://ihl-databases.icrc.org/ihl/full/GCIII-commentary [hereinafter ICRC Commentary] ("It is generally accepted that cyber operations having similar effects to classic kinetic operations would amount to an international armed conflict.").

[93] *See infra* ¶¶ 7–8.

[94] *See* Jack Stubbs & Christopher Bing, *Hacking the Hackers: Russian Group Hijacked Iranian Spying Operation, Officials Say,* REUTERS (Oct. 20, 2019, 9:24 PM), https://www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1X00AK.

an international armed conflict remains a subject of debate. A cyber operation causing an immediate physical effect comparable to that of a traditional kinetic attack could trigger an IAC.

5. An international armed conflict exists where there is an armed conflict between two States, even if one or both of the parties does not recognize that there is an ongoing armed conflict.[95] According to the ICTY's *Tadić* case, it also exists when an "organized armed group that is under the 'overall control' of one State engages in hostilities against another State."[96] In the latter case, although the conflict involves a non-State actor, the conflict is internationalized due to the "overall control" of a State over the group.[97] A State exercises the required degree of control over an organized group when it "has a role in organizing, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group."[98] The Council of Advisers noted that this may be particularly relevant for cyber operations where a State directs a cyber operation by a non-State actor against another State. However, the "overall control" test does not apply in the case of individuals or a group that is insufficiently organized.[99] In order to attribute to a State the conduct of individuals or groups not organized into a military structure, the individuals or group must receive from that State

---

[95] Geneva Convention III, *supra* note 81, art. 2. *See also* TALLINN MANUAL 2.0, *supra* note 37, at 379-380.

[96] TALLINN MANUAL 2.0, *supra* note 37, at 380. *See also Prosecutor v. Tadić*, Case No. IT-94-1-A, Appeals Chamber Judgment, ¶ 137 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999) [hereinafter *Tadić* Appeals Chamber Judgment] (explaining the "overall control" test); *Lubanga* Judgment, *supra* note 87, ¶ 541 (endorsing the "overall control" test as the correct approach for determining if an armed conflict has become "internationalized").

[97] *Lubanga* Judgment, *supra* note 87, ¶ 541.

[98] *Tadić* Appeals Chamber Judgment, *supra* note 96, at ¶ 137. The ICJ in the *Nicaragua* Case has used the standard of "effective control," which was further endorsed in the ICJ's *Bosnia v. Serbia* Case; *Nicaragua* Case, *supra* note 50, at ¶¶ 105-115 (June 27); Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. Rep. 43, ¶ 400 (Feb. 26). For a discussion of the "overall control" test versus the "effective control" test, *see* Antonio Cassese, *The* Nicaragua *and* Tadić *Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia*, 18 EUR. J. INT'L LAW 649, 649-68 (2007). There are two interrelated issues here, one of which has to do with establishing whether the armed conflict was international or non-international, and the other of which pertains to State attribution.

[99] TALLINN MANUAL 2.0, *supra* note 37, at 382.

specific instructions or subsequent public approval of the conduct at issue.[100] Applying the "overall control" test, the Council of Advisers agreed with the Tallinn Manual assessment that "if one State exercises overall control over an organized group of hackers that penetrates another State's cyber infrastructure and causes significant physical damage, the armed conflict qualifies as 'international' in nature."[101] The Council of Advisers acknowledged that these issues exacerbate the already existing challenges, discussed above, regarding attribution in a cyber context. In addition to disguising their behavior, States can outsource cyber activity to "black-hat" hackers,[102] who can be difficult to trace individually[103] and even more difficult to link back to State officials giving orders.[104] In practice, this may prove to be a considerable challenge in the regulation and prosecution of cyber misconduct.

6. What remains unclear is the threshold of violence of hostilities required to trigger an IAC. One approach considers an international armed conflict to exist wherever there is resort to armed force between States, with no requirement as to intensity or duration,[105] while the competing view requires a higher level of intensity in order to reach the level of an IAC, and is thus more limiting.[106] Under the second view, an individual cyber act resulting only in limited damage or injury would not necessarily trigger an IAC.[107] Regardless of the required threshold, the ultimate determination is a factual one to be resolved on a case by case basis.[108]

---

[100] *See id.*

[101] *Id.* at 381. *See also* ICRC Commentary, *supra* note 92, at ¶ 306.

[102] Black-hat hackers are those who violate computer security for the sake of personal gain, malice, or other illicit purposes. They can be compared with white-hat hackers, which are those who draw attention to vulnerabilities in computer systems for the purpose of protection and strengthening cybersecurity systems. *See* JAMES A. O'BRIEN & GEORGE M. MARAKAS, MANAGEMENT INFORMATION SYSTEMS 536-37 (10th ed. 2011).

[103] Chaumette, *supra* note 90, at 24–25.

[104] *See id.* at 25.

[105] *See Tadić* Decision on the Defense Motion, *supra* note 87, ¶ 70. *See also* International Committee of the Red Cross, *COMMENTARY ON THE FIRST GENEVA CONVENTION: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* ¶ 236 (Knut Dörmann et al. eds., 2016).

[106] *See* Jann N. Kleffner, *Scope of Application of International Humanitarian Law*, *in* THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 43, 45 (Dieter Fleck ed., 3d ed. 2013).

[107] TALLINN MANUAL 2.0, *supra* note 37, at 383–84.

[108] *Id.* at 384.

7. The Council of Advisers disagreed as to whether or not it would be beneficial to maintain a higher threshold for triggering an IAC.[109] Based on the definition of armed conflict as use of force between two States, members advocating the higher threshold argued that any attack that produced only non-physical effects could not constitute use of force, and therefore could not trigger an IAC. A cyber operation that produced a sufficiently immediate secondary physical effect, however, could trigger an IAC. The Council of Advisers also considered that States may be reluctant to consider non-kinetic cyber operations as "armed" and to initiate an armed conflict, because such an approach could lead to an increase in the number of armed conflicts due to the high number of non-kinetic cyber operations occurring at present.

Whether Cyber Operations Can Trigger Non-International Armed Conflict

Because of the additional condition of intensity and organization, a cyber operation or attack is likely to trigger a NIAC only in exceptional circumstances.

8. In the context of a non-international armed conflict, an additional element must be considered when determining whether or not a cyber operation could trigger an armed conflict. For a NIAC to exist, there must be "protracted armed violence between governmental authorities and organized armed groups or between such groups within a State."[110] Drawing on *Tadić*—beyond the threshold discussed in the previous subsection—in order to qualify as a NIAC, cyber operations must amount to a minimum level of intensity, and the non-State armed group involved must also achieve a minimum degree of organization.[111] According to both Additional Protocol II and the Rome Statute, "situations of internal

[109] *See* Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Human Rights Council, U.N. Doc. A/HRC/44/38 ¶ 16 (asserting that the dominant view is that there exists some threshold between an isolated strike and an IAC).

[110] *Tadić* Decision on the Defense Motion, *supra* note 87, ¶ 70. Further, unlike Additional Protocol II, which requires the organized armed group(s) to exert control over a part of the territory, the Rome Statute has no such requirement for finding the existence of a NIAC. *See Bemba* Decision, *supra* note 86, ¶ 236.

[111] *See, e.g.,* Prosecutor v. Milošević, Case No. IT-02-54-T, Decision on Motion for Judgment of Acquittal, ¶¶ 16-17 (Int'l Crim. Trib. for the Former Yugoslavia June 16, 2004) [hereinafter

disturbances and tensions, such as riots, isolated and sporadic acts of violence or other acts of a similar nature"[112] do not meet the threshold of violence to qualify as NIACs.[113] In order to ascertain whether the threshold of "protracted armed violence" has been met, the ICTY has considered factors such as "the gravity of the attacks and their recurrence, the number of victims, the temporal and territorial expansion of violence,"[114] as well as "the collective character of hostilities,"[115] weapons used by parties to the conflict,[116] and whether the conflict attracts the attention of and action on the part of the Security Council.[117] Given the high threshold for "protracted armed violence," the Council of Advisers agreed with the Tallinn Manual assessment that "network intrusions, the deletion or destruction of data (even on a large scale), computer network exploitation, and data theft,"[118] or the blockage of Internet functions and services, would not on their own amount to a non-international armed conflict.[119] The Council

---

Milošević Decision on Motion]. *See also* TALLINN MANUAL 2.0, *supra* note 37, at 387 (noting that *Tadić* Decision on the Defense Motion implicitly sets out two criteria for qualification as a NIAC: (1) intensity of the hostilities and (2) involvement of an organized group).

[112] Rome Statute, *supra* note 16, art. 8(2)(d).

[113] *See id.*; *see also* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts art. 1(2), June 8, 1977, 1125 U.N.T.S. 609 [hereinafter Additional Protocol II]. *See also* Robin Geiss, *Cyber Warfare: Implications for Non-international Armed Conflicts*, 89 INT'L L. STUD. 627, 632 (2013).

[114] *Milošević* Decision on Motion, *supra* note 111, ¶¶ 28-29. *See also* Geiss, *supra* note 113, at 632-33.

[115] Prosecutor v. Limaj, Case No. IT-03-66-T, Trial Chamber Judgment, ¶¶ 94-134 (Int'l Crim. Trib. for the Former Yugoslavia Nov. 30, 2005) [hereinafter *Limaj* Trial Chamber Judgment]. *See also* Geiss, *supra* note 113, at 633.

[116] Prosecutor v. Mrkšić, Case No. IT-95-13/1-T, Trial Chamber Judgment, ¶ 407 (Int'l Crim. Trib. for the Former Yugoslavia Sept. 27, 2007) [hereinafter *Mrkšić* Trial Chamber Judgment]; *Limaj* Trial Chamber Judgment, *supra* note 115, ¶ 90; *Milošević* Decision on Motion, *supra* note 111, ¶¶ 31-32. *See also* TALLINN MANUAL 2.0, *supra* note 37, at 388.

[117] *Mrkšić* Trial Chamber Judgment, *supra* note 116, ¶ 421; Prosecutor v. Ntaganda, ICC-01/04-02/06, Judgment, ¶ 716 (July 8, 2019) [hereinafter *Ntaganda* Judgment]; Prosecutor v. Ongwen, ICC-02/04-01/15, Trial Judgment, ¶ 2684 (Feb. 4, 2021). For an even more expansive list, s*ee also* Prosecutor v. Haradinaj, Case No. IT-04-84*bis*-T, Retrial Judgment, ¶¶ 394, 170 (Int'l Crim. Trib. for the former Yugoslavia Nov. 29, 2012). *See also* TALLINN MANUAL 2.0, *supra* note 37, at 388.

[118] TALLINN MANUAL 2.0, *supra* note 37, at 388.

[119] *Id. See also* ICRC Commentary, *supra* note 92, at ¶ 471 ("[C]ertain cyber operations may not have a similar impact to that of kinetic attacks but be limited to blocking internet functions, exploiting networks, or stealing, deleting or destroying data. If cyber operations consist exclusively of the latter kind of acts, the intensity of violence as required under humanitarian

further agreed that a cyber operation would likely be required to cause physical damage or injury (and/or potentially incapacitation, in the view of some) in order to rise to the intensity level required for a NIAC. As to the requirement that the violence be "protracted," this may be met by "[f]requent, albeit not continuous, cyberattacks . . . occurring within a relatively well-defined period."[120]

9. In addition to the intensity requirement, for a non-international armed conflict to exist, there must be at least one non-State organized armed group engaged.[121] According to the Tallinn Manual, a group is considered "armed" if it has the capacity to undertake cyber operations.[122] As to organization, a group meets the NIAC requirements if it has "some degree of organization and the ability to plan and carry out sustained military operations."[123] The Council of Advisers agreed with the Tallinn Manual assessment that cyber operations and military computer attacks by private individuals or small, loosely-connected groups of hackers would not meet the organization requirement.[124] Beyond that, whether a group is sufficiently organized is a factual determination to be made on a case-by-case basis.[125] The Council also noted that a group organized entirely online would be difficult, if not impossible, to classify as having met the organization requirement.[126] Although the fact that a group did not physically meet would not alone prevent a group from satisfying the organizational requirement,[127] having a purely virtual group would make it almost impossible to determine group membership without extensive forensic investigations because of the difficulty of tracing who is behind

---

law is unlikely to be reached.").

[120] TALLINN MANUAL 2.0, *supra* note 37, at 389.

[121] *Id.*

[122] *Id.*

[123] Prosecutor v. Lubanga, ICC-01/04-01/06, Decision on the confirmation of charges, ¶ 233 (Jan. 29, 2007); *see also Limaj* Trial Chamber Judgment, *supra* note 115, ¶ 129. *See also* TALLINN MANUAL 2.0, *supra* note 37, at 389 (noting that a group is "organized" if "it is under an established command structure and can conduct sustained military operations.").

[124] TALLINN MANUAL 2.0, *supra* note 37, at 389.

[125] *Id.*

[126] *See* ICRC Commentary, *supra* note 92, at 471 ("However, for a group that only organizes online it may be difficult – yet arguably not impossible – to determine whether it meets the threshold of organization required to become a Party to a non-international armed conflict.").

[127] TALLINN MANUAL 2.0, *supra* note 37, at 390.

each computer.[128] Further, the geographic spread of members of a virtual group means it would be far more difficult to effectively implement a group strategy due to the limited ability of such a group to enforce orders.[129] Thus, the Council of Advisers found it hard to imagine a virtual group meeting the organizational requirement for a non-international armed conflict. The Council of Advisers agreed with the Tallinn Manual assessment that, due to the intensity and organizational requirements, cyber operations alone will amount to NIAC only in exceptional circumstances.[130]

Nexus Between Criminal Act and Armed Conflict

There must exist a nexus between a cyber operation and armed conflict to constitute a War Crime under Article 8 of the Rome Statute.

10. The Elements of Crimes require that a criminal act "took place in the context of and was associated with" an armed conflict.[131] The ad hoc tribunals have interpreted this requirement to mean that an act must be sufficiently related to hostilities and the armed conflict must have played a significant role in the accused's decision and ability to perpetrate the crime.[132] However, the crime need not have taken place during battle, as IHL applies to the whole of the territory of the parties engaged in hostilities, and the conflict need not be the

---

[128] Geiss, *supra* note 113, at 636.

[129] *Id.* at 636-37.

[130] TALLINN MANUAL 2.0, *supra* note 37, at 385-86. *See also* Geiss, *supra* note 113, at 629.

[131] Elements of Crimes, *supra* note 70, at 18. *See also* KNUT DÖRMANN, ELEMENTS OF WAR CRIMES UNDER THE ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT 26-28 (2003).

[132] Prosecutor v. Kunarac, Case No. IT-96-23 & IT-96-23/1-A, Appeals Chamber Judgment, ¶¶ 58-59 (Int'l Crim. Trib. for the Former Yugoslavia June 12, 2002) [hereinafter *Kunarac*]. *See also* Prosecutor v. Ntaganda, ICC-01/04-02/06 OA5, Judgment on the appeal of Mr. Ntaganda against the "Second decision on the Defence's Challenge to the jurisdiction of the Court in respect of Counts 6 and 9," ¶ 68 (June 15, 2017) [hereinafter *Ntaganda* Judgment on appeal] (endorsing the *Kunarac* multi-factor approach to determining the nexus between a criminal act and an armed conflict for the purposes of constituting a war crime); Situation in the Islamic Republic of Afghanistan, ICC-02/17-138 OA4, Judgment on the appeal against the decision on the authorization of an investigation into the situation in the Islamic Republic of Afghanistan, ¶ 69 (March 5, 2020) [hereinafter *Situation in Afghanistan*] (also endorsing the *Kunarac* multi-factor approach). *See also* SCHABAS, *supra* note 64, at 235.

perpetrator's primary motivation for the commission of criminal conduct.[133] The Appeals Chamber of the ICTY assessed the following factors to determine if a crime was sufficiently related to a conflict: "the fact that the perpetrator is a combatant; the fact that the victim is a non-combatant; the fact that the victim is a member of the opposing party; the fact that the act may be said to serve the ultimate goal of a military campaign; and the fact that the crime is committed as part of or in the context of the perpetrator's official duties."[134]

11. Thus, a cyber operation must have a nexus to an armed conflict in order for it to potentially constitute a war crime. This nexus may capture extra-territorial crimes, not solely those linked to the territory of the conflict, provided that it is otherwise sufficient.[135] The Council of Advisers agreed that the above factors could be used to assess whether or not a cyber operation is sufficiently related to a conflict to constitute a war crime under Article 8 of the Rome Statute.

Attacks

Cyber operations can amount to "attacks" under traditional IHL and the Rome Statute.

12. The Council of Advisers discussed the meaning of the term "attack" within Additional Protocol I (AP I) and the Rome Statute and how it may be applied in a cyber context.[136] The meaning of "attack" is critical because many IHL rules stemming from the core IHL principles, such as distinction and proportionality, only apply to cyber operations that qualify as attacks. Neither the Rome Statute nor the Elements of Crimes define the

---

[133] *Kunarac*, *supra* note 132, ¶¶ 58-60; *Situation in Afghanistan*, *supra* note 132, ¶ 69 (endorsing *Kunarac*). *See also* SCHABAS, *supra* note 64, at 235.

[134] *Kunarac*, *supra* note 132, ¶ 59. *See also Ntaganda* Judgment on appeal, *supra* note 132, ¶ 68 (quoting *Kunarac*); *Situation in Afghanistan*, *supra* note 132, ¶ 69 (quoting *Kunarac*).

[135] *See* Situation in the Islamic Republic of Afg., ICC-02/17-138 OA4, Judgment on appeal, (Mar. 5, 2020) (authorizing an investigation into alleged war crimes related to the situation in Afghanistan even when the alleged conduct occurred outside of Afghanistan and when the victims of the alleged acts were captured outside of Afghanistan).

[136] It is important to note that the term attack, as discussed here by the Council of Advisers, is distinct from use of force that would trigger an armed conflict *jus in bello* and also distinct from "armed attack" under a *jus ad bellum* analysis.

term "attack."[137] Therefore, the ICC has relied upon the definition in Additional Protocols I and II.[138] Article 49(1) of Additional Protocol I defines the term "attack" as "acts of violence against the adversary, whether in offence or in defence."[139] By this definition, violence is what distinguishes "attacks" from other military operations, meaning that cyber operations that are by their nature non-violent, such as espionage or psychological operations, cannot be considered attacks.[140] According to the Tallinn Manual, the principle that "acts of violence" include acts with violent consequences, not just acts that are themselves violent, is well settled in international humanitarian law.[141] As such, the Tallinn Manual defines a cyberattack as "a cyber operation . . . that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[142] AP I also accounts for the neutralization of a military objective in Article 52(2), that would in effect "destroy" the objective.[143] In a cyber context, disrupting or halting the functions of a State's critical infrastructure or jamming military capabilities, even if the critical infrastructure or military hardware is not physically destroyed, may qualify as an attack under IHL (although not necessarily a war crime).[144]

13. The Council of Advisers noted that the concept of an attack under AP I and Rome Statute Article 8 may be broader than the armed attack required to trigger armed conflict. For example, cyber operations that cause a loss of function or meaningfully disrupt a system might constitute an attack, but not armed attack. Some members of the Council suggested that, in

---

[137] *See* Prosecutor v. Bosco Ntaganda, Separate opinion of Judge Howard Morrison and Judge Piotr Hofmański on the Prosecutor's appeal, ICC-01/04-02/06-2666-Anx1 (Mar. 30, 2021); *see also* SCHABAS, *supra* note 64, at 256.

[138] *See id.*

[139] Additional Protocol I, *supra* note 82.

[140] *See* TALLINN MANUAL 2.0 *supra* note 37, at 415; Julia Dornbusch, *Das Kampfführungsrecht im internationalen Cyberkrieg* (2017), 155.

[141] *See* TALLINN MANUAL 2.0 *supra* note 37, at 415

[142] *Id*.

[143] *See* Additional Protocol I, *supra* note 82, art. 52 ¶ 2; Ambos, *supra* note 69, at 124.

[144] *See* Ambos, *supra* note 69, at 124; INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS 41 (2015) [hereinafter ICRC, CHALLENGES]; International Committee of the Red Cross, *International Humanitarian Law and Cyber Operations During Armed Conflicts: ICRC Position Paper*, 7-8 (Nov. 2019) [hereinafter ICRC, Position Paper]; Tim McCormack, *International Humanitarian Law and the Targeting of Data*, 94 INT'L L. STUD. 222 (2018).

particular, an operation designed to disable a computer or network qualifies as an attack under IHL, regardless of whether the computer or network is disabled by traditional kinetic means or cyber ones.

14. In their discussion of objects protected from attack under IHL, the Council of Advisers discussed data as an intangible but protected object. Members of the Council agreed that civilian data is protected under IHL, discussing in particular a cyber operation altering or deleting civilian medical data which should be considered a violation of IHL, and therefore possibly a war crime.[145] The Council noted that States have come out against cyber operations targeting healthcare systems, particularly in the midst of the COVID-19 pandemic.[146] Such attacks may amount to violations of IHL and international criminal law.[147] This concept diverges somewhat from the Tallinn Manual where the majority of experts specifically excluded data from the category of "objects" under IHL as it is currently understood,[148] though the Tallinn Manual does note that personal medical data should be protected.[149] Some members of the Council suggested that in select instances the data on a computer and the system that operates on a computer might be more important than the physical object itself and so should receive protection.

---

[145] *See* Ambos, *supra* note 69, at 43; ICRC, Position Paper, *supra* note 144.

[146] *See generally* statements made by States during the first round of informal meetings of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (June 15–19, 2020) and during the UN Security Council Arria-Formula Meeting on Cyber Attacks Against Critical Infrastructure (August 26, 2020).

[147] OXFORD INST. FOR ETHICS, LAW & ARMED CONFLICT, *The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector*, https://elac.web.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea (last visited Oct. 11, 2020); OXFORD INST. FOR ETHICS, LAW & ARMED CONFLICT, *The Second Oxford Statement on International Law Protections of the Healthcare Sector During COVID-19: Safeguarding Vaccine Research*, https://elac.web.ox.ac.uk/article/the-second-oxford-statement (last visited Oct. 11, 2020).

[148] *See* TALLINN MANUAL 2.0 *supra* note 37, at 437; *cf.* Ambos, *supra* note 69, at 131 ("From a modern perspective the difference between physical and virtual objects becomes, at least in the cyber context, blurred; therefore, data should, in principle, be covered by the protection.").

[149] *See* TALLINN MANUAL 2.0 *supra* note 37, at 515.

SECTION III

Application of Core IHL Principles to Cyberwarfare

The core principles of IHL, including distinction and proportionality, apply in a cyber context. Thus, the relevant paragraphs within Article 8 of the Rome Statute implicating these principles also apply in a cyber context.

15. Because of the close connection between war crimes and the core principles of IHL, it is relevant to consider how those principles apply to cyber operations in order to understand how Article 8 of the Rome Statute applies to cyberwarfare. The principles of distinction and proportionality are of particular importance.[150] The Council of Advisers' deliberations and considerations are discussed in the following section.

Principle of Distinction

The principle of distinction applies in the context of cyber operations.

16. The distinction between civilians and combatants is crucial within the IHL framework and, consequently, crucial to determining whether an attack qualifies as a war crime in armed conflict.[151] Under IHL, it is prohibited to direct attacks against civilians and civilian objects; conversely, attacks may only be directed against military objectives.[152] According to

---

[150] The principle of precautions may also be relevant, although it was not discussed by the Council. Under IHL and customary international law, the principle of precautions, which is enshrined in AP I art. 57 and is considered to apply in both IAC and NIAC, provides that precautions must be taken to avoid or minimize incidental civilian loss and damage to civilian objects in the course of a military attack. *See* International Committee of the Red Cross, *Rule 15. Principle of Precautions in Attack,* IHL-Databases, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule15. In the context of a cyber operation, the principle of precautions may require that the head of a cyber operation not only sufficiently map the potential effects of a cyber operation, particularly on civilians and civilian objects, but also take precautions to avoid or mitigate those potential effects. *See* Eric Talbot Jensen, *Cyber Attacks: Proportionality and Precautions in Attack*, 89 INT'L L. STUD. 198, 210-211 (2013).

[151] *See* Ambos, *supra* note 69, at 130. *See also* Rome Statute, *supra* note 16, Art. 8 ¶ 2 (b) (i), 8 ¶ 2 (e) (i).

[152] Additional Protocol I, *supra* note 82, arts. 48, 51 and 52; HENCKAERTS & DOSWALD-

Article 52(2) of Additional Protocol I, military objectives are defined as "objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization in the circumstances ruling at the time, offers a definite military advantage."[153] Determining whether an object is a military objective is a context-based decision, made on a case-by-case basis.[154] As discussed in the previous section, the Council of Advisers diverged from the Tallinn Manual's understanding that data is not an object, ultimately arguing that civilian data may in some ways be more valuable than the physical computer or device housing that data. In particular, the Council of Advisers referenced the importance of protecting civilian medical data.[155]

17. A key challenge for application of the principle of distinction in cyberwarfare is the fact that civilian and military computer systems are often interconnected, and cyber infrastructure is commonly subject to dual use.[156] Militaries often rely heavily on civilian cyber infrastructure to support and execute operations and even use social media platforms, such as Twitter or Facebook.[157] Dual-use cyber infrastructure serves both civilian and military functions,[158] but since status as a military objective according to the applicable definition supersedes the protection of a civilian object, even dual-use facilities and networks may be legally characterized as military objectives.[159] As such, there are many cyber operations that take place on dual-use cyber networks that would be difficult to classify as violating the principle of distinction.[160] However, too broad an application of this

---

BECK, *supra* note 70, at 3-8, 25-29.

[153] Additional Protocol I, *supra* note 82, art. 52 ¶ 2.

[154] *See* Ambos, *supra* note 69, at 131.

[155] It is important to note that the Tallinn Manual 2.0 does account for special protections of personal medical data. *See* TALLINN MANUAL 2.0 *supra* note 37, at 515.

[156] *See* Ambos, *supra* note 69, at 130; Droege, *supra* note 91, at 562–66.

[157] *See* Ambos, *supra* note 69, at 132; Dornbusch, *supra* note 140, at 168.

[158] The Tallinn Manual likened a dual-use cyber network to a network of roads used by civilians and military personnel. *See* TALLINN MANUAL 2.0 *supra* note 37, at 446.

[159] *Id.* at 445.

[160] *See* Ambos, *supra* note 69, at 132. However, there is a view that cyberspace is designed with a high level of redundancy, meaning that one of its characteristics is the ability to immediately re-route data traffic. According to this view, the in-built resilience should be considered when assessing whether the target's destruction or neutralization would offer a definite military advantage, as required by the AP I, Art. 52(2) definition of a military objective. If this definition

definition of military objective may have broad consequences. For example, it could lead to the determination that large social media platforms, such as the ones mentioned above, or even the Internet as a whole, could become military objectives if parties to a conflict are using them for military purposes.[161] It has been suggested that the definition of military objective should be construed narrowly, such that attacks should identify and target the specific components or segments used for military action.[162] The Tallinn Manual further suggests that the circumstances under which the entire Internet would become subject to attack are highly unlikely.[163] The Council of Advisers agreed with the Tallinn Manual assessment that "as a legal and practical matter, virtually any attack against the Internet would have to be limited to discrete segments thereof"[164] in order to comply with IHL.

18. An additional issue related to the principle of distinction as applied in cyberwarfare comes from AP I Article 51(4), which prohibits indiscriminate attacks.[165] This covers both attacks that are conducted in an indiscriminate manner—in other words, an attack not directed specifically at a military objective—and attacks conducted by means and methods of warfare incapable of being directed at a specific military objective.[166] The former can include a discriminate weapon that is used indiscriminately, such as a piece of malware triggered by accessing a website used by both civilian and military actors.[167]

19. The Council of Advisers agreed with the Tallinn Manual assessment that the latter—i.e. means and methods of warfare that are by their nature indiscriminate either because they cannot be directed toward a specific military objective or because their effects cannot be contained—are prohibited.[168]

---

is not met, the object would remain civilian and may not be attacked. *See further* the ICRC 2015 Challenges Report, p. 69. International humanitarian law and the challenges of contemporary armed conflicts, INTERNATIONAL REVIEW OF THE RED CROSS 69 (2015).

[161] *See* TALLINN MANUAL 2.0 *supra* note 37, at 446.

[162] Droege, *supra* note 91, at 563–66.

[163] *See id.*

[164] *Id*. *See also* Additional Protocol I, *supra* note 82, art. 51 ¶ 5 (a) on treating multiple distinct military objectives as a singular military objective.

[165] Additional Protocol I, *supra* note 82, Art. 51 ¶ 4.

[166] *See id.*

[167] *See* TALLINN MANUAL 2.0 *supra* note 37, at 468.

[168] *See id.*, at 455–56; *see also* Additional Protocol I, *supra* note 82, Art. 51 ¶ 4; Rome Statute,

However, the ICC cannot presently prosecute the war crime of use of "indiscriminate weapons." The Rome Statute lists the use of indiscriminate weapons as a war crime in Article 8(2)(b)(xx) (covering an IAC) but states that this applies only to weapons "included in an annex to this Statute;" yet, there is no annex.[169] States Parties might want to consider either amending the Rome Statute to create the required annex or delete the requirement of having an annex so that the Rome Statute conforms with IHL. Despite this lacuna in the Rome Statute, the ICC has noted that indiscriminate attacks may qualify as intentional attacks against the civilian population or individual civilians[170] and that Article 8(2)(e)(i) may encompass attacks that are carried out in an indiscriminate manner.[171] On this approach, certain indiscriminate attacks using cyber means and methods of warfare could also qualify as the war crime of attacking civilian objects under Article 8(2)(b)(ii). States Parties might additionally want to consider amending the Rome Statute to include the war crime of using indiscriminate weapons (with a completed annex or no annex requirement) if committed during a NIAC.

20. Whether or not effects can be contained is a relevant concern for cyber operations. Some of the more advanced cyber operations in recent years, such as the Stuxnet virus where a malicious computer worm targeted an Iranian uranium enrichment facility,[172] have produced effects beyond their intended target.[173] The Council of Advisers also agreed with the Tallinn Manual assessment that where a cyber operation targeting a

---

supra note 16, Art. 8 ¶ 2 (b) (xx).

[169] For an explanation of why the Rome negotiations resulted in an annex requirement but no annex, *see* Roger S. Clark, *Building on Article 8(2)(b)(xx) of the Rome Statute of the International Criminal Court: Weapons and Methods of Warfare*, 12 NEW CRIM. L. REV. 366 (2009).

[170] Prosecutor v. Katanga, ICC-01/04-01/07, Judgment pursuant to article 74 of the Statute, ¶ 802 (Mar. 7, 2014) [hereinafter Prosecutor v. Katanga, Judgment].

[171] *Ntaganda* Judgment, *supra* note 117, ¶ 921 (providing the example of a perpetrator (1) who targets an area, as opposed to a specific object, and (2) who is aware of the presence of civilians in the relevant area as constituting an indiscriminate attack that would be covered by Article 8(2)(e)(i)).

[172] David Sanger, *Obama Order Sped up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), https://nytimes.com/2012/06/01/world/middleast/obama-ordered-wave-of-cyberattacks-agaisnt-iran.html.

[173] Though the target of the Russian NotPetya cyber operation was Ukraine, the wiper attack spread throughout the world, damaging thousands of networks and crippling operations of several major companies, amounting to $10 billion in damages. *See* Greenberg, *supra* note 58.

dual-use system could have targeted the specific components in use by the military alone, an attack on the system as a whole is prohibited, and, therefore, violators of the prohibition could face criminal responsibility under Rome Statute Article 8.[174]

Principle of Proportionality

The principle of proportionality applies in the context of cyber operations. Both direct and indirect consequences must be considered in a proportionality calculation.

21. The principle of proportionality "sets limits to the use of means and methods of warfare and in particular prohibits causing 'superfluous injury or unnecessary suffering' and 'widespread, long-term and severe damage to the environment.'"[175] According to AP I, an attack that violates the principle of proportionality is one which may be expected to cause incidental damage to civilian objects, injury to civilians, or loss of civilian life that would be "excessive in relation to the concrete and direct military advantage anticipated."[176] The principle of proportionality likewise appears in Article 8(2)(b)(iv) of the Rome Statute.[177] Of particular salience is that AP I Article 51(5)(b) uses the language of "excessive" whereas Rome Statute Article 8(2)(b)(iv) refers to "clearly excessive." This difference in language means that certain acts may be grave breaches under AP I Article 85(3)(b) but would not amount to a war crime under Rome Statute Article 8. Such acts do, however, constitute war crimes under the domestic legislation of many States, including numerous common law States that have adopted "Geneva Convention Acts," which implement their obligations under the Geneva Conventions and AP I.[178]

---

[174] *See* TALLINN MANUAL 2.0, *supra* note 37, at 470; Dornbusch, *supra* note 140, at 176.

[175] Ambos, *supra* note 69, at 134.

[176] Additional Protocol I, *supra* note 82, art. 51 ¶ (5) (b).

[177] Rome Statute, *supra* note 16, art. 8 ¶ 2 (b) (iv) ("Intentionally launching an attack in the knowledge that such attack will cause 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.").

[178] *See* International Committee of the Red Cross, *National Implementation of IHL*, IHL-Databases, https://ihl-databases.icrc.org/applic/ihl/ihl-nat.nsf/vwLawsByCountry.xsp?

22. It is important to note that the principle of proportionality specifically allows for incidental civilian harm, but this damage must be proportionate to the expected military advantage.[179] Assessment of both incidental civilian harm and military advantage are anticipatory and thus require judgment based on all reasonably available information at the time of planning, approval, and execution of an attack.[180]

23. In a cyber context, according to Tallinn Manual Rule 113 on proportionality, a cyber operation that "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated is prohibited."[181] Because cyber operations are sometimes launched through civilian infrastructure, they may cause incidental civilian harm "both during transit and because of the [cyber operation] itself."[182] Both forms of incidental civilian harm must be considered when launching a cyber operation and both must conform to the principle of proportionality.[183] Additionally, the Council of Advisers agreed that anticipated collateral damage should cover both direct damage resulting from a cyber operation and also indirect effects of a cyber operation, although these effects may be more difficult to accurately anticipate[184] and would still need to meet Rome Statute intent requirements.[185]

24. The Council of Advisers accepted that the requirement that cyber operations adhere to the principle of proportionality helps to offset the limitations of the principle of distinction.[186] Because the principle of distinction is practically

---

xp_topicSelected=GVAL-992BU6.

[179] *See* Ambos, *supra* note 69, at 134; *see also* TALLINN MANUAL 2.0 *supra* note 37, at 471.

[180] *See* TALLINN MANUAL 2.0, *supra* note 37, at 474–75. *See also* Wolff Heintschel von Heinegg, *Considerations of Necessity under Article 57(2)(a)(ii), (c), and (3) and Proportionality under Article 51(5)(b) and Article 57(2)(b) of Additional Protocol I*, *in* NECESSITY AND PROPORTIONALITY IN INTERNATIONAL PEACE AND SECURITY LAW (Claus Kreß & Robert Lawless eds., 2020); Stefan Oeter, *Specifying the Proportionality Test and the Standard of Due Precaution: Problems of Prognostic Assessment in Determining the Meaning of "May Be Expected" and "Anticipated," in* NECESSITY AND PROPORTIONALITY IN INTERNATIONAL PEACE AND SECURITY LAW (Claus Kreß & Robert Lawless eds., 2020).

[181] *Id.* at 470.

[182] *Id.* at 471.

[183] *Id.*

[184] *See* Ambos, *supra* note 69, at 135; *see also* TALLINN MANUAL 2.0 *supra* note 37, at 472.

[185] See *supra* Part I, Section III.

[186] *See* Ambos, *supra* note 69, at 134; Droege, *supra* note 91, at 566.

limited in the context of dual-use networks, as discussed above, requiring that incidental civilian harm expected to be caused by an attack on a dual-use system or network must not be excessive to the anticipated military advantage, creates a potentially important outer limit for cyber operations.[187] Even so, States Parties should also consider amending the Rome Statute to include a counterpart for Article 8(2)(b)(iv) in NIAC in order to give recognition to the crime of disproportionate attacks in NIAC, which would bring the Rome Statute into line with customary international law[188] and could encompass indiscriminate cyber operations when committed in NIAC.

SECTION IV: CONCLUSION

25. Based on their discussion, the Council of Advisers agreed that in the event of an ongoing international or non-international armed conflict, cyber operations may constitute war crimes if they satisfy the general requirements as laid out in the introduction to this chapter, and if they constitute one of the enumerated crimes in Article 8(2)(a) – (e) of the Rome Statute.[189] However, there remain several challenges and open questions based on the nature of cyber conduct, some relevant to each of the Rome Statute's enumerated crimes and others particular to Article 8.

26. One open question—particular to application of Article 8 and explored in the previous sections—is whether or not a cyber operation can itself trigger an international armed conflict and, therefore, the application of IHL. The Council of Advisers did not reach consensus on the IAC threshold question, though some seemed to favor a higher threshold, with some reservations.[190] In considering this issue, the Council of Advisers recognized that in applying basic principles of international law in a cyber context, legal experts are confronted with the question of whether to take a broad or restrictive approach.[191] The Council of Advisers emphasized that any approach taken

---

[187] *See* Ambos, *supra* note 69, at 134.

[188] *See* International Committee of the Red Cross, *Rule 14. Proportionality in Attack*, IHL-Databases, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule14#Fn_A9C8FAD0_00023.

[189] Beyond qualifying as an enumerated act in Article 8, such acts must also be charged as part of a case against a person which reaches the ICC's gravity threshold for admissibility. *See* Rome Statute, *supra* note 16, art. 17 ¶ 1 (d).

[190] *See supra* Part II, Section II, ¶¶ 6–7 (discussing the threshold for an IAC).

[191] *See* Yoram Dinstein, *Computer Network Attacks and Self-Defense, in* 76 INT'L L. STUDIES,

should reflect a desire to maximize protections for civilians.

27. The Council of Advisers noted that an alleged war crime must occur in the context of an armed conflict by the time the acts relevant to an ICC trial are committed. However, especially in circumstances where a cyber act is the event that initiates an armed conflict, as part of the preliminary examination into alleged war crimes, the Office of the Prosecutor would need to establish there is a reasonable basis to believe that a conflict exists. The Council of Advisers noted that this creates complications because at this stage, the Prosecutor has limited investigative powers to obtain information. In this instance, States would need to provide any information they possessed following a cyber operation initiating a conflict on a voluntary basis. The Council of Advisers agreed that this presents a considerable challenge considering the hesitancy on the part of States to share information on cyber operations.

28. In the discussion of objects that are protected from attack under IHL, the Council of Advisers opted to take a somewhat broader approach than that of the Tallinn Manual to include civilian data, particularly civilian medical data. The Council determined that because of the particular and growing importance of data in digitized societies, it should be included as a protected object, at least in certain circumstances.[192] However, given the language of Rome Statute Article 8, this expansion would be applied differently in the context of an IAC versus a NIAC. If civilian data is considered a civilian object, under Rome Statute Article 8(2)(b)(ii), it would be a war crime to attack it, unless it becomes a military objective, in the context of an IAC.[193] However, there does not appear to be an

---

COMPUTER NETWORK ATTACK AND INT'L LAW 99, 105 (Michael N. Schmitt and Brian T. O'Donnell eds., 2002). A report by NATO's Cooperative Cyber Defense Center called the offensive cyber operation, Stuxnet, which led to the physical destruction of centrifuges in Iran's Natanz nuclear facility, a clear violation of Article 2(4) but experts could not agree whether it rose to the level of an armed attack. *See* Kim Zetter, *Legal Experts: Stuxnet Attack on Iran was Illegal 'Act of Force,'* WIRED (Mar. 25, 2013), https://www.wired.com/2013/03/stuxnet-act-of-force/. The Council also considered that the approach to applying principles of the *jus ad bellum* framework in a cyber context, particularly whether a cyber act could constitute "use of force" under UN Charter Article 2(4) or an "armed attack" under Article 51, should be fairly restrictive, in an effort to prevent further conflict so that the threshold for using self-defense in response under Article 51 of the UN Charter is not inappropriately triggered.

[192] *See e.g.* ICRC, CHALLENGES, *supra* note 144, at 43.

[193] Rome Statute, *supra* note 16, art. 8 ¶ 2 (b) (ii).

analogous crime of attacking civilian objects in Article 8(2)(e), which applies to NIAC.[194] The Council noted that this issue may need more clarification, ideally through interpretation by the ICC, or amendments to the Rome Statute.

29. Though the Council of Advisers unanimously agreed that the core IHL principles of distinction and proportionality apply to cyber operations, the practical application of such principles remains open to question and discussion. Some of the discussion was covered in Section III of this chapter and much of the discussion is also covered in previous projects, such as the Tallinn Manual. One significant difference is that while the use of "indiscriminate" weapons is banned under IHL, as detailed above, until Rome Statute Article 8(2)(b)(xx) is amended, this war crime cannot be prosecuted at all before the ICC—and even then, unless the Statute is amended, only in an IAC. The Council of Advisers agreed that many of the questions will only be resolved with additional State practice and potential jurisprudence by the ICC and other international and national bodies.

30. In their discussions, the Council of Advisers also touched upon open questions and outstanding issues relevant to each of the enumerated crimes in the Rome Statute based on the nature of cyber conduct. In particular, the Council discussed the ways that challenges in attribution and identifying intent of a particular cyber operation may create complications for application of Rome Statute Article 8. Though attribution will become easier with time and technological advancements, it remains a challenge, particularly when it comes to assigning individual criminal responsibility.[195] As stated earlier in this chapter and in the chapters on the crime of genocide and crimes against humanity, States may attempt to disguise their cyber conduct[196] or may outsource cyber activity, which can be difficult to track[197]

---

[194] Rome Statute, *supra* note 16, art. 8 ¶ 2 (e). This, however, does not mean that attacks against civilian objects are not prohibited. Attacks against civilian objects are prohibited under the law of NIACs. *See* Study on customary international humanitarian law: A contribution to the understanding and respect for the rule of law in armed conflict, INTERNATIONAL REVIEW OF THE RED CROSS (2020), rule 7 (and various military manuals cited within); *Tadić* Decision on the Defense Motion, *supra* note 87, ¶ 127. It is important to note that other war crimes may exist or come into existence under international law beyond the Rome Statute, including customary international law, and national law.

[195] *See* Chaumette, *supra* note 90, at 5.

[196] *See* Stubbs & Bing, *supra* note 94.

[197] *See* Chaumette, *supra* note 90, at 23–25.

and even more difficult to link back to a State.[198] Some cyber operations may involve numerous actors.[199] Because cyber operations may have wide-reaching unintended consequences, [200] it may be difficult to discern whether a specific target was intended or merely incidental civilian damage. Although Article 8 accounts for incidental damage that is clearly excessive in relation to an expected military advantage in Article 8(2)(b)(iv) and through the principle of proportionality, it may be more difficult to establish the intent required for war crimes under Article 8(2)(b)(i)-(iii), among others.

31. Similar concerns may also create challenges in identifying the required nexus between a criminal act and ongoing armed conflict. For example, if one cannot accurately attribute an attack to the alleged perpetrator, it will be difficult to assess what role the armed conflict played in the perpetrator's decision to carry out an attack.[201] Similarly, attribution and intent difficulties can complicate the requirement that a perpetrator have knowledge of the existence of armed conflict.[202] In particular, the Council of Advisers considered that if cyber activity is outsourced by a party to the conflict, as a factual matter, it may be more difficult to establish that the perpetrators of a particular attack had knowledge that there was an ongoing armed conflict, particularly if that attack is launched from territory outside of the territory of conflict.

32. The Council of Advisers agreed that many of these questions will have to be left to State practice or to the ICC and other international and national legal bodies for interpretation and clarification. As technology continues to advance and cyber operations become an increasingly important tool for both State and organizational actors, the ICC will likely have occasion to address some of the questions raised and to give clarity on the application of Rome Statute Article 8 on War Crimes in the context of cyber operations and cyberwarfare.

---

[198] *See id.* at 25.

[199] *See id*.

[200] *See* Greenberg, *supra* note 58 (recalling that NotPetya was "likely more explosive than even its creators intended.").

[201] *See* SCHABAS, *supra* note 64, at 235 (noting that the armed conflict must play a substantial role in the perpetrator's decision or ability to commit the crime, or in the manner of committing it).

[202] *See* Elements of Crimes, *supra* note 70, at Introduction to Article 8.

PART III

The Application of Article 7 (Crimes Against Humanity) of the Rome Statute to Cyberwarfare

PART III: THE APPLICATION OF ARTICLE 7 (CRIMES AGAINST HUMANITY) OF THE ROME STATUTE TO CYBERWARFARE

SECTION I

Crimes Against Humanity at the International Criminal Court: General Overview

Crimes against humanity are set out in Article 7 of the Rome Statute.[203] Notably, Article 7 does not require conduct to have a nexus to an armed conflict in order to constitute a crime against humanity.[204] Crimes against humanity may occur at any time, including during times of peace or civil strife, thus permitting the ICC to respond to large-scale atrocities committed against civilians.[205]

Article 7 defines crimes against humanity, for the purposes of the Rome Statute, as the commission of certain prohibited acts "as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack."[206] The acts in question must fall into one of the enumerated acts listed in Article 7(1): murder, extermination, enslavement, deportation, imprisonment, torture, rape or sexual violence, persecution, enforced disappearance, apartheid, and other inhumane acts.[207] Given the limitations of Article 22 of the Rome Statute, which

---

[203] *See* Rome Statute, *supra* note 16, art.7.

[204] Elements of Crimes, *supra* note 70; *see also* Otto TRIFFTERER & KAI AMBOS, THE ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT: A COMMENTARY, 155 (3rd ed. 2016); *see also* Darryl Robinson, *Defining 'Crimes Against Humanity' at the Rome Conference*, 93 AM. J. INT'L L. 43 (1999).

[205] *See* Robinson, *supra* note 204, at 46; *see also* TRIFFTERER & AMBOS, *supra* note 204, at 155.

[206] Rome Statute, *supra* note 16, art. 7(1).

[207] As provided in art. 7(1) Rome Statute, these enumerated acts are:

> (a) Murder; (b) Extermination; (c) Enslavement; (d) Deportation or forcible transfer of population; (e) Imprisonment or other severe deprivation of physical liberty in violation of fundamental rules of international law; (f) Torture; (g) Rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilization, or any other form of sexual violence of comparable gravity; (h) Persecution against any identifiable group or collectivity on political, racial, national, ethnic, cultural, religious, gender as defined in

requires that "the definition of a crime shall be strictly construed and shall not be extended by analogy,"[208] to constitute a crime against humanity, cyber conduct must qualify as one of the enumerated acts already listed in Article 7(1).[209]

Contextual Elements

In order to constitute a crime against humanity, an act, including a cyber operation, must be part of a collective act that satisfies the contextual elements deriving from Article 7(1) and the definition of attack provided for in Article 7(2).[210] As stated above, the chapeau of Article 7(1) stipulates that to qualify as a crime against humanity, an attack must be "committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack."[211] Article 7(2)(a) specifies that an attack directed against any civilian population "means a course of conduct involving the multiple commission of acts referred to in paragraph 1 against any civilian population, pursuant to or in furtherance of a State or organizational policy to commit such attack."[212] Combining these two provisions, courts have identified five contextual elements for crimes against humanity.[213] These elements are: "(i) an attack directed against any civilian population; (ii) a State or organizational policy; (iii) an attack of a widespread or systematic nature; (iv) a nexus exists between the individual act and the attack; and (v) knowledge of the attack."[214]

> paragraph 3, or other grounds that are universally recognized as impermissible under international law, in connection with any act referred to in this paragraph or any crime within the jurisdiction of the Court; (i) Enforced disappearance of persons; (j) The crime of apartheid; (k) Other inhumane acts of a similar character intentionally causing great suffering, or serious injury to body or to mental or physical health.

[208] *Id.* art. 22(2).

[209] *Id.* art. 7(1).

[210] *See* SCHABAS, *supra* note 64, at 153.

[211] Rome Statute, *supra* note 16, art. 7(1).

[212] *Id.* art. 7(2)(a).

[213] SCHABAS, *supra* note 64, at 153.

[214] Situation in the Republic of Côte d'Ivoire, ICC-02/11, Corrigendum to "Decision Pursuant to Article 15 of the Rome Statute on the Authorization of an Investigation into the Situation in the Republic of the Côte d'Ivoire," ¶ 29 (Nov. 5, 2011); SCHABAS, *supra* note 64, at 153.

SECTION II

The following section reflects the Council of Advisers' discussion of when cyber conduct may meet the five contextual elements to constitute a crime against humanity as enumerated in Article 7(1) of the Rome Statute.

Attack Directed against Any Civilian Population

A cyber operation with physical and/or violent effects may qualify as an attack based on traditional interpretations of the word. A cyber operation with non-physical effects may qualify as an attack under the crimes against humanity framework if it constitutes one of the enumerated acts in Article 7(1), particularly those with non-physical elements. A cyber operation will be considered against the civilian population if civilians were the primary object of the attack.

1. Article 7(2) specifies that an "attack" means "a course of conduct involving the multiple commission of acts" referred to in Article 7(1) "against any civilian population." An "attack" need not be specifically a military attack,[215] rather, an attack may constitute a "campaign or operation carried out against the civilian population".[216] That is, Article 7(2) requires there be a series or overall flow of events as opposed to an aggregate of random or unconnected acts or a single isolated act.[217] For an "attack" to have occurred, all that is needed is the commission of the acts referred to in Article 7(1) pursuant to or in furtherance of a State or organizational policy as required by Article 7(2). An attack may involve any form of violence or mistreatment against a civilian population that falls under Article 7(1).[218] An attack can be, but need not be, an armed attack or even part of an armed conflict.

---

[215] *See* Elements of Crimes, *supra* note 70, at Introduction to Article 7, ¶ 3.

[216] *See* Prosecutor v. Jean-Pierre Bemba, ICC-01/05-01/08-3343, Judgment Pursuant to Article 74 of the Statute, ¶ 149 (Mar. 21, 2016) [hereinafter *Bemba*, Judgment] (internal citation omitted).

[217] *See* Prosecutor v. Katanga, Judgment, *supra* note 170, ¶ 1101 (Mar. 7, 2014); *see also* Prosecutor v. Laurent Gbagbo, ICC-02/11-01/11-656-Red, Decision on the Confirmation of Charges Against Laurent Gbagbo, ¶ 209 (June 12, 2014) [hereinafter Gbagbo, Decision on the Confirmation of Charges].

[218] *See* Prosecutor v. Katanga, Judgment, *supra* note 170, ¶ 1101.

2. The meaning of "civilian population" is not clear from the text of Article 7(1), nor is it defined in Article 7(2), allowing for some flexibility in interpretation. Generally, the ICC adopts the traditional international humanitarian law (IHL) definition of "civilian population"[219] whether or not an alleged crime took place in or during an armed conflict.[220] The word "any" confirms that "civilian population" is intended to be broadly construed. "Any civilian population" is therefore made up of individuals, regardless of nationality, ethnicity, or other distinguishing feature, as "persons who are civilians as opposed to members of armed forces or other legitimate combatants."[221] Consistent with IHL, during a time of armed conflict, the presence in the civilian population of individuals such as combatants who do not come within the definition of civilian does not deprive the population of its civilian character.[222] A person is to be considered a civilian if there is a doubt about his or her status. The requirement that the attack be "directed against" the civilian population means that the attack must target the civilian population.[223] It does not require that the *entire* population of a State or territory be under attack, but the number of individuals targeted must be sufficient to establish the attack was directed at the population rather than "a limited and randomly selected number of individuals."[224] When considering whether a civilian population has been the primary object of an attack, international courts and tribunals have considered, *inter alia*, "the means of attack, the status of the victims, their number, the discriminatory nature of the attack, the nature of the crimes committed in its course, the resistance of assailants at the time and the extent to which the attacking force may be said to have complied or attempted to comply with the laws of war."[225] When an attack occurs during

---

[219] See Additional Protocol I, *supra* note 82, art. 50(2); HENCKAERTS & DOSWALD-BECK, *supra* note 70, at 5.

[220] *See* Rosa Ana Alija Fernández & Jaume Saura Estapà, *Towards a Single and Comprehensive Notion of 'Civilian Population' in Crimes against Humanity*, 16 INT'L CRIM. L. REV. 1, 20 (2016).

[221] *See, e.g., Bemba* Decision, *supra* note 86, at ¶ 78 (citing *Kunarac*, *supra* note 132, ¶ 90); *see also* Prosecutor v. Katanga, Judgment, *supra* note 170, ¶ 1102.

[222] Additional Protocol I, *supra* note 82, art. 50(3); *see also Bemba*, Judgment, *supra* note 216, at ¶153.

[223] *See* Prosecutor v. Bosco Ntaganda, Public redacted version of Judgment on the appeal of Mr Bosco Ntaganda against the decision of Trial Chamber VI of 7 November 2019 entitled 'Sentencing judgment,' ICC-01/04-02/06-2666-Red (Mar. 30, 2021)

[224] *Kunarac*, *supra* note 132, ¶ 90.

[225] *See id.* ¶ 92; *see also, e.g., Bemba*, Judgment, *supra* note 216, at ¶ 153.

the course of an armed conflict, it is unnecessary to demonstrate that the victims are linked to any particular side in the attack.[226]

3. The Council of Advisers agreed that multiple cyber operations amounting to at least one of the enumerated acts in Article 7(1) could constitute an "attack" for the purposes of Article 7. The Council, however, was not in agreement as to whether or not such an attack must have a physical effect on the population or whether the impact could be non-physical or psychological. Some members of the Council asserted that since an attack is any form of "violence" falling under article 7(1), this implies a required physical component, which would preclude many forms of cyber conduct from qualifying as enumerated acts. However, other members believed that the crimes against humanity framework, unlike others under the Rome Statute, allows for crimes with non-physical effects. Additionally, Advisers noted that though an attack has been understood to mean violence against the civilian population, the term "violence" is not explicitly stated in the statute, and there are enumerated crimes, such as apartheid or persecution, which do not necessarily require violence. Furthermore, jurisprudential interpretations of an attack as requiring (physical) violence may merely reflect the particular facts of cases previously brought before tribunals. Cybercrimes brought before tribunals may very well be interpreted differently. Finally, members of the Council argued that because the Rome Statute specifically mentions mental health and because the Elements of Crimes refer to mental health in its discussion of "other inhumane acts" and "torture," a non-physical impact appears possible for attacks taking the form of those enumerated acts.[227] The Council of Advisers agreed that it remains unclear whether a cyber operation with a non-physical impact would rise to the level of an "attack" for some of the other enumerated acts.[228]

---

[226] *See* TRIFFTERER & AMBOS, *supra* note 204, at 175.

[227] Rome Statute, *supra* note 16, art. 7(1)(k); Elements of Crimes, *supra* note 70, art. 7(1)(k); Prosecutor v. Francis Kirimi Muthaura, Uhuru Muigai Kenyatta, and Mohammed Hussein Ali, ICC-01/09-02/11, *Decision on the Confirmation of Charges pursuant to Article 61(7)(a) and (b) of the Rome Statute,* ¶ 279 (Jan. 23 2012).

[228] It is also important to note that a cyber operation would need to be charged as part of a case which reaches the Article 17(1)(d) gravity threshold in order to be admissible in the ICC. It is not currently clear if an attack with non-physical effects would itself reach this threshold. Prosecutor v. Al Hassan, 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*,' ICC-01/12-01/18-601-Red OA, ¶ 59 (Feb. 19, 2020).

4. With regard to attacks directed at a civilian population, the Council of Advisers noted that civilians must be targeted by the attack. This would distinguish the targeted population of a crime against humanity from collateral damage from an attack.

State or Organizational Policy

Cyber operations backed either by States or non-State organized entities may fulfil the contextual element of State or organizational policy assuming that a policy can be either explicitly shown or inferred based on conduct. One may infer the existence of a policy based on cyber conduct.

5. In order to constitute a crime against humanity, a cyber operation must be linked to a State or an organization.[229] As stated in Article 7(2), an attack under Article 7 must be conducted "pursuant to or in furtherance of a State or organizational policy to commit such attack." Although the meaning of "State" appears to be self-evident, and would include the conduct of its regional or local organs attributed to it under international law, the Council of Advisers acknowledged that there is some debate as to the exact meaning of "organizational." In particular, there is disagreement as to whether "organizational" refers only to (1) State-like organizations or (2) any organization with the capacity to carry out such attacks regardless of whether or not it is affiliated with a State.[230] Adhering more closely to the second view, the ICC Pre-Trial and Trial Chambers have consistently held that groups having control over a specific territory and organizations with the capacity to commit a

---

[229] *See* Elements of Crimes, *supra* note 70, at Introduction to Article 7, ¶ 3 (noting that "policy to commit an attack" requires that the *State or organization* actively promote or encourage an attack) (emphasis added).

[230] *See e.g.* Tilman Rodenhäuser, *Beyond State Crimes: Non-State Entities and Crimes against Humanity*, 27 LEIDEN J. OF INT'L L. 913, 921–22 (2014); Charles Chernor Jalloh, *What Makes a Crime Against Humanity a Crime Against Humanity*, 28 AM. U. INT'L L. REV. 381 (2013); Claus Kreß, *On the Outer Limits of Crimes Against Humanity: The Concept of Organization Within the Policy Requirement: Some Reflections on the March 2010 ICC Kenya Decision*, 23 LEIDEN J. INT'L L. 855 (2010); Claus Kreß, *Some Reflections on the International Legal Framework Governing Transnational Armed Conflicts*, 15 J. CONFLICT & SECURITY L. 245 (2010); William A. SCHABAS, *State Policy as an Element of International Crimes*, 98 J. CRIM. L. & CRIMINOLOGY 953 (2008).

widespread or systematic attack against the civilian population qualify for the purposes of Article 7(2).[231] That is, the organization must "have sufficient resources, means and capacity to bring about the course of conduct or the operation" and "a set of structures or mechanisms, whatever those may be, that are sufficiently efficient to ensure the coordination necessary to carry out an attack."[232] According to the Trial Chamber in *Katanga*, this does not mean that the organization must be so structured as to assume the characteristics of a State—what is important are the organization's capacities for action, mutual agreement and coordination.[233] That said, the majority of the Pre-Trial Chamber in *Prosecutor v. Uhuru Muigai Kenyatta* rejected the argument that "only State-like organizations may qualify" within the meaning of Article 7(2)(a), finding that "the formal nature of a group and the level of its organization should not be the defining criterion. Instead…a distinction should be drawn on whether a group has the capacity to perform acts which infringe on basic human values." Alternatively, Judge Hans-Peter Kaul, in a dissenting opinion suggested that an organization must have State or quasi-State abilities to be capable of committing crimes against humanity for purposes of the Rome Statute.[234] Another Pre-Trial Chamber, in the *Ruto* Case, has concurred with the majority view and also given further guidance. It held that when determining whether a particular group can be an "organization", the Chamber may take into account several factors, including among others: "i) whether the group is under responsible command, or has an established hierarchy; ii) whether the group possesses, in fact, the means to carry out a widespread or systematic attack against a civilian population iii) whether the group exercises control over part of the territory of a State; iv) whether the group has criminal activities against the civilian population as a primary

---

[231] *See* Gbagbo, Decision on the Confirmation of Charges, *supra* note 217, ¶217.

[232] Prosecutor v. Katanga, Judgment, *supra* note 170, ¶ 1119.

[233] *See id.*, ¶1120.

[234] *See* Prosecutor v. William Samoei Ruto, Henry Kiprono Kosgey and Joshua Arap *Sang*, ICC-01/09-01/11, Dissenting Opinion by Judge Hans-Peter Kaul to Pre-Trial Chamber II's Decision on the Prosecutor's Application for Summons to Appear for William Samoei Ruto, Henry Kiprono Kosgey and Joshua Arap Sang, ¶ 49–51 (Mar. 15, 2011); *See also* Prosecutor v. Francis Kirimi Muthaura, Uhuru Muigai Kenyatta, and Mohammed Hussein Ali, ICC-01/09-02/11, Dissenting Opinion by Judge Hans-Peter Kaul, ¶ 12 (Mar. 15, 2011).

purpose; v) whether the group articulates, explicitly or implicitly, an intention to attack a civilian population; vi) whether the group is part of a larger group, which fulfills some or all of the above mentioned criteria."[235] While there has been no authoritative pronouncement by the Appeals Chamber,[236] the findings of the Pre-Trial and Trial Chambers as well as the work of authoritative bodies such as the International Law Commission (ILC) and the writings of publicists confirm the view that both State-like and non-State like organizations would fall within the meaning of "organizations."[237] Both types of groups, affiliated with the State or not, may engage in cyber operations that would meet the requirements of Article 7(2).[238] In this regard, the Council of Advisers noted that this is the same view that guided negotiations on the Rome Statute. Accepting this majority view of the Pre-Trial and Trial Chambers, it can be argued that a loosely organized group of hackers would probably not meet the organizational requirement,[239] but a structured and stable group of hackers that in fact has the capacity to perform acts infringing on basic human values would.[240] Indeed, in the context of the Kenya Situation, an ICC Pre-Trial Chamber confirmed charges of crimes against humanity in relation to suspects associated with a loose "network" of opposition politicians affiliated with different political groups as well as media and the police.[241] Additionally, the Council of Advisers agreed that the ability to engage in cyber operations could potentially help establish the organized nature of the entity or demonstrate that it has the resources or capacity to commit the type of widespread or systematic attacks with which Article 7 is concerned. This would be consistent with the current ICC jurisprudence since, according to the rulings

[235] Prosecutor v. Ruto, Decision on the Confirmation of Charges Pursuant to Article 61(7)(a) and (b) of the Rome Statute, ICC-01/09-01/11, ¶ 185 (Jan. 23, 2012) [hereinafter Ruto, Decision on the Confirmation of Charges]; Situation in the Republic of Kenya, *supra* note 36, ¶ 93.

[236] *See* Prosecutor v. Bosco Ntaganda, Separate opinion of Judge Luz Del Carmen Ibáñez Carranza on Mr Ntaganda's appeal, ICC-01/04-02/06-2666-Anx3, ¶ 39 ff.; Prosecutor v. Bosco Ntaganda, Partly concurring opinion of Judge Chile Eboe-Osuji, ICC-01/04-02/06-2666-Anx5, ¶ 138 ff.

[237] INTERNATIONAL LAW COMMISSION, DRAFT ARTICLES ON PREVENTION AND PUNISHMENT OF CRIMES AGAINST HUMANITY, WITH COMMENTARIES 39–42 (2019).

[238] *See* SCHABAS, *supra* note 64, at 161 (noting that it is possible that private individuals or groups or organizations that are not 'state-like' could commit 7(2) crimes, as there has been no authoritative pronouncement on the matter).

[239] *See* Ambos, *supra* note 69, at 142.

[240] *See* Chaumette, *supra* note 90, at 21.

[241] Ruto, Decision on the Confirmation of Charges, *supra* note 235, ¶¶ 184–86.

cited above, organizations would only need to fulfill some, not all, of the criteria to be capable of committing cyber operations. Though the Council of Advisers agreed that an organized non-State entity with the proper resources could be considered "organizational" under this element, the Council of Advisers similarly acknowledged that today, State or State-backed entities maintain the most advanced cyber capabilities and have been responsible for the most severe cyber operations.

6. Neither Article 7 nor the Elements of Crimes define the term "policy," leaving the term open to interpretation. The Elements of Crimes merely state that a policy to commit an attack requires that the State or organization behind the act actively promotes or encourages an attack against the civilian population.[242] In "exceptional circumstances," such a policy may be implemented through the deliberate failure to act where the inaction is consciously aimed at encouraging an attack.[243] Such a policy may not be inferred solely from the absence of governmental or organizational action, however.[244] There must be evidence of planning, direction or organization sufficient to show the act was not an instance of spontaneous or isolated violence.[245]

7. Several cases at the ICC have addressed the policy element. For example, in order to prove the existence of a policy according to the *Katanga* Judgment, it is not necessary to show that "a State or organization adopted and disseminated a pre-established design or plan to that effect."[246] It only needs to be shown that the entity concerned meant to commit an attack against a civilian population. The existence of a policy may be inferred from conduct, taking into consideration a variety of factors such as whether "(i) the attack was planned, directed or organized; (ii) a recurring pattern of violence; (iii) the use of public or private resources to further the policy; (iv) the involvement of the State or organizational forces in the commission of crimes; (v) statements, instructions or documentation attributable to the State or the organization condoning or encouraging the commission of crimes; and/or (vi) an underlying motivation."[247] The Council of Advisers noted that cyber

---

[242] *See* Elements of Crimes, *supra* note 70, at Introduction to Article 7, ¶ 3.

[243] *See id*, ¶ 3, n.6.

[244] *See id.*

[245] *See Bemba* Decision, *supra* note 86, ¶81; *see also* Ruto, Decision on the Confirmation of Charges, *supra* 235, ¶ 211.

[246] Prosecutor v. Katanga, Judgment, *supra* note 170, ¶ 1109.

[247] *Bemba*, Judgment, *supra* note 216, ¶ 160; Prosecutor v. Katanga, Judgment, *supra* note

operations, themselves, might serve as evidence of a number of these factors. For example, an organization could use private resources to pay hackers to engage in cyber operations that are used to conduct one of the enumerated acts under Article 7(1). Members of the Council further recalled that although there must be a link between a course of conduct and the policy, a perpetrator need not necessarily be motivated by the policy or be a member of either the State or organization, so long as there is evidence the perpetrator engaged in conduct envisaged by the policy and had knowledge of the policy's existence.[248] Thus, the Council of Advisers concluded that an independent hacker or group of hackers would still be covered under the Statute even if they were not part of the State government or independent organization responsible for the underlying policy.

Attack of a Widespread or Systematic Nature

A cyber operation, on its own, or in the context of other conduct, could rise to the threshold of a widespread or systematic attack, necessary to establish a crime against humanity.

8. The *chapeau* element required for an attack to be considered a crime against humanity must be either widespread or systematic in nature.[249] The terms "widespread" and "systematic" are not defined in the Rome Statute. ICC jurisprudence indicates that "widespread" refers to the large-scale nature of the attack and the number of victims, and that the attack may be "massive, frequent, carried out collectively with considerable seriousness and directed against a multiplicity of victims."[250] It is also the case that a single act, committed by an individual, can constitute the prohibited underlying act(s) of a crime against humanity so long as it takes place within the context of a broader attack against any civilian population pursuant to or in furtherance of a State or organizational policy. Nonetheless, the assessment of the widespread nature of the attack is not exclusively quantitative or geographical and must be carried out on the basis of the

---

162, ¶ 1109.

[248] *Bemba*, Judgment, *supra* note 216, ¶ 161.

[249] *See* TRIFFTERER & AMBOS, *supra* note 204, at 166.

[250] *Bemba*, Judgment, *supra* note 216, ¶ 163.

individual facts.[251] In order to establish the widespread nature of an attack, jurisprudence considers the number of victims (though no particular number of victims is required), the extent of the geographical area affected, and the duration of the attack.[252] The Council of Advisers agreed that because of the "deterritorialization" of many cyber operations, the geographical element could be inapplicable in relation to the place where the effects of the attack are felt but the geographic origins of the attack would be relevant in establishing their widespread nature.[253] However, the Council of Advisers unanimously agreed that a cyber operation could be considered widespread, thereby meeting the threshold of this chapeau element. As with physical attacks, cyber operations that are the result of a single inhumane act of great magnitude would also qualify. That said, rather than focusing on the extent of the geographical area affected, judges could instead consider the number of servers or the extent of civilian infrastructure, such as a power grid or sanitation facilities, targeted by the attack and the damage resulting therefrom.[254]

9. "The term, 'systematic' pertains to the organized nature of the acts of violence and to the improbability of their random occurrence."[255] The systematic character of an attack refers to the "existence of 'patterns of crimes' reflected in the non-accidental repetition of similar criminal conduct on a regular basis."[256] An attack has also been found to be systematic when "the perpetrators employed similar means and methods to attack the different locations."[257] Given the systemized nature of cyber conduct,

---

[251] *See* Gbagbo, Decision on the Confirmation of Charges, *supra* note 217, ¶ 223.

[252] *See* Chaumette, *supra* note 90, at 21; *see also* Prosecutor v. Ntaganda, ICC-01/04-02/06-309, Decision Pursuant to Article 61(7)(a) and (b) of the Rome Statute on the Charges of the Prosecutor Against Bosco Ntaganda, ¶ 24 (June 14, 2014); *see also* Prosecutor v. Ongwen, ICC-02/04-01/15-422-Red, Decision on the confirmation of charges against Dominic Ongwen, ¶ 65 (Mar. 23, 2016). Note that the same criteria are used in Art. 14.4 of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[253] *See* Chaumette, *supra* note 90, at 21.

[254] *See id.*

[255] Prosecutor v. Al Bashir, ICC-02/05-01/09-3, Decision on the Prosecution's Application for a Warrant of Arrest against Omar Hassan Ahmad Al Bashir, ¶ 81 (Mar. 4 2009) [hereinafter Bashir 2009 Decision]; Prosecutor v. Katanga, Judgment, *supra* note 170, ¶ 1123.

[256] Prosecutor v. Katanga, Judgment, *supra* note 170, ¶ 1123.

[257] Prosecutor v. Ntaganda, Decision on the Prosecutor's Application under Article 58, ICC-01/04-02/06-36-Red, ¶ 31 (Jul. 13, 2012).

the Council of Advisers unanimously agreed that a cyber operation could qualify as systematic. While acknowledging that cyber operations may have unintended and even somewhat random consequences, cyber operations often involve repeated patterns that speak to a certain systematic nature. The Council of Advisers even suggested that the use of cyber operations could constitute evidence of a systematic nature in the context of additional non-cyber conduct.

10. The Council of Advisers further recalled that it is the overall attack that must be widespread or systematic, not the specific acts with which the accused is charged.[258] Thus, an isolated cyber operation could still constitute a crime against humanity so long as it is in the context of other acts that together would form a widespread and systematic attack sufficient for the threshold of the crime.

Nexus between the Individual Act and the Underlying Attack

A cyber operation must itself constitute the underlying attack or must be established, via a nexus, as a part of a widespread or systematic attack.

11. Because the individual act must be committed as part of a widespread or systematic attack, there must be a nexus between the enumerated acts in Article 7(1) and the overall attack directed against the civilian population.[259] The Council of Advisers specified that an individual cyber operation should be part of an enumerated act that was committed in furtherance of a widespread and systematic attack against the civilian population in order for the cyber operation to constitute a crime against humanity.[260] In determining whether such a cyber operation forms part of the widespread attack, the ICC would consider "the characteristics, the aims, the nature or consequences of the [enumerated] act"[261] of which it

---

[258] *See* SCHABAS, *supra* note 64, at 165.
[259] Prosecutor v. Katanga, Judgment, *supra* note 170, ¶ 1124.
[260] Prosecutor v. Katanga, ICC-01/04-01/07, Decision on the Confirmation of Charges, ¶ 400 (Sept. 30, 2008).
[261] *Bemba* Decision, *supra* note 86, ¶ 86.

forms a part. In the instance of a cyber operation that itself would constitute the widespread and systematic attack, the nexus is already clear. Isolated cyber operations, however, that differ in their nature, aims and consequences from other acts that form part of an attack would fall outside the ambit of Article 7.[262]

Knowledge of the Attack

Establishing specific criteria for knowledge under Article 7 will likely be more difficult in the context of cyber operations than in other instances of crimes against humanity.

12. Article 7(1) requires that the underlying acts must be committed with knowledge of the attack. The knowledge element forms part of the Elements of Crimes for the various enumerated acts, requiring that the perpetrator of an attack "knew that the conduct was part of or intended the conduct to be part of a widespread systematic attack against a civilian population."[263] Having "knowledge" of the attack does not however require the perpetrator to have "knowledge of all characteristics of the attack or the precise details of the plan or policy of the State or organization."[264] Further, "in the case of an emerging widespread or systematic attack against a civilian population . . . the mental element is satisfied if the perpetrator intended to further an attack."[265] The specific content of the required knowledge and its object of reference are disputed.[266] Specifically, it is unclear whether the Rome Statute's definition of knowledge in Article 30 should be read as following the approach taken by some other international tribunals that "knowledge of the attack" also includes the lower *mens rea* standard that an accused was aware or willfully blind, willingly accepted, or knowingly took the risk that his or her actions would

---

[262] *See* Prosecutor v. Katanga, Judgment, *supra* note 170, ¶ 1124.

[263] Elements of Crimes, *supra* note 70, at art. 7(1)(h), ¶ 6 (discussing the crime against humanity of persecution); *see also id.* at art. 7(1)(k), ¶ 5 (discussing the crime against humanity of other inhumane acts).

[264] Elements of Crimes, *supra* note 70, at Introduction to Article 7, ¶ 2.

[265] *Id.*

[266] *See* TRIFFTERER & AMBOS, *supra* note 204, at 176.

be part of an attack.[267] With these requirements in mind, the Council of Advisers agreed that in a cyber context, the perpetrator accused of the cyber operation would have to know that their actions formed part of an underlying widespread attack against the civilian population.[268] Past Tribunals have inferred knowledge, which may be proven circumstantially. Given the nature of cyber operations, the Council of Advisers concluded that knowledge may in some circumstances be harder to establish in a cyber context than in the case of more traditional, physical attacks against the population.

SECTION III

13. If a cyber operation meets all of the contextual requirements, it would still have to qualify as one of the enumerated acts listed in Article 7(1) in order to constitute a crime against humanity. A cyber operation could qualify as a new means of committing one of the traditional constitutive acts listed in Article 7(1). While many of the enumerated acts could be conducted through cyber-enabled means, the Council of Advisers considered that torture, persecution, apartheid, and other inhumane acts may be relevant for cyber operations as they do not require physical violence directed at a civilian population.[269]

---

[267] *See* Prosecutor v. Sainović, Case No. IT-05-87-A, Judgment, ¶ 267–71 (Int'l Crim. Trib. for the Former Yugoslavia Jan. 23, 2014) (affirming the Trial Chamber's holding that the *mens rea* requirement could be met by an individual taking the risk of his acts being part of an attack against a civilian population); *Kunarac*, *supra* note 132, ¶ 102; Prosecutor v. Blaškić, Case No. IT-95-14-T, Judgment, ¶ 251 (Int'l Crim. Trib. for the Former Yugoslavia Mar. 3, 2000); Prosecutor v. Tadić, Case No. IT-94-1-T, Opinion and Judgment, ¶ 657 (Int'l Crim. Trib. for the Former Yugoslavia May 7, 1997). Compare to Rome Statute, *supra* note 16, art. 30(3) ("For the purposes of this article, 'knowledge' means awareness that a circumstance exists or a consequence will occur in the ordinary course of events."). *See also* GUÉNAËL METTRAUX, 2 INTERNATIONAL CRIMES: CRIMES AGAINST HUMANITY 350–51 (2020) ("Lastly, it is unclear whether, in proceedings before the ICC, the risk-taking standard of *mens rea* concerning the accused's part in the attack would apply. Absent an express exclusion of this possibility in the Statute or the *Elements*, and consistent with the view that the drafters sought to adhere to existing law, it could reasonably be suggested that the ICC regime has absorbed this lowered standard of *mens rea* in relation to the question of the accused's awareness of his participation in the attack."). The view was expressed that this interpretation is a complete misunderstanding of Article 38 and its preparatory work.

[268] *See* METTRAUX, *supra* note 267, at 349–50.

[269] The Council of Advisers noted, however, that any acts with either physical or non-physical

14. Assuming that the five contextual elements discussed above[270] were met, the Council of Advisers determined that cyber operations might be used to carry out acts with exclusively physical effects such as murder and extermination. Similar to the crime of genocide discussed in the next chapter, a cyber operation could produce a mass casualty event by, for example, shutting down the cooling system of a nuclear power plant and exposing the civilian population to radioactive materials.[271] Or cyber operations could be used to manipulate or shut down dams or waterworks causing potentially deadly flooding.[272] Again, similar to the crime of genocide, with respect to extermination, cyber operations could be used to create conditions of life "calculated to bring about the destruction of part of a population."[273] For example, cyber actors could cut the power grid for a significant period of time over a severely cold winter[274] or cut off access to medical services by disrupting the networks in local hospitals. Furthermore, cyber operations could be used to delete or alter medical records to deprive civilians from receiving care that they need.[275] Whereas genocide can in some respects be an inchoate crime, and it is the special mental requirement that is the crux of the crime (see next chapter), for the crime against humanity of extermination, extermination (i.e., mass killing) would actually need to occur.

15. Article 7(2)(e) defines torture as, "the intentional infliction of severe pain or suffering, whether physical or mental, upon a person in the custody or under the control of the accused."[276] The inclusion of mental pain or suffering is consistent with the 1984 UN Convention Against Torture and Other Inhuman or Degrading Treatment or Punishment, which states that:

---

effects must reach the ICC's gravity threshold under Article 17(1)(d).

[270] *See supra* Part III Section 1.

[271] *See* Marco Roscini, *Gravity in the Statute of the International Criminal Court and Cyber Conduct That Constitutes, Instigates or Facilitates International Crimes*, 30 CRIM. L.F. 247, 250 (2019).

[272] *See id.* at 261.

[273] Rome Statute, *supra* note 16, art. 7(2)(b).

[274] *See* Roscini, *supra* note 271, at 261; Cyber operations targeting a national power grid have already taken place in Ukraine, just before Christmas in 2016. *See* Andy Greenberg, *New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction,* WIRED (Sept. 12, 2019, 11:55 AM), https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/.

[275] *See* Roscini, *supra* note 271, at 266.

[276] Rome Statute, *supra* note 16, art. 7(2)(e).

> 'torture' means any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person for such purposes as obtaining from him or a third person information or a confession, punishing him for an act he or a third person has committed or is suspected of having committed, or intimidating or coercing him or a third person, or for any reason based on discrimination of any kind, when such pain or suffering is inflicted by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity. It does not include pain or suffering arising only from, inherent in or incidental to lawful sanctions.[277]

Based on the above, the Council of Advisers considered that it is likely that cyber operations can be used to inflict psychological torture on civilians. Recently, Nils Melzer, the UN's special rapporteur on torture and other cruel, inhuman or degrading treatment or punishment commented that "[c]ybertechnology can also be used to inflict, or contribute to, severe mental suffering while avoiding the conduit of the physical body, most notably through intimidation, harassment, surveillance, public shaming and defamation, as well as appropriation, deletion or manipulation of information."[278] Members of the Council of Advisers agreed with Melzer's assessment that cyber torture of this nature could cause high levels of anxiety and depression, feelings of isolation, and even heightened risk of suicide[279] and could therefore qualify, assuming all of the contextual elements were met, as a crime against humanity under Article 7(1)(f).

16. Per Article 7(2)(g), persecution in the context of crimes against humanity is "the intentional and severe deprivation of fundamental rights contrary to international law by reason of the identity of the group or collectivity."[280] Importantly, fundamental rights have never been defined, though courts

---

[277] Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment art. 1, *opened for signature* Dec. 10, 1984, 1465 U.N.T.S. 85 (entered into force June 26, 1987) [hereinafter Convention against Torture].

[278] *See* Owen Bowcott, *UN Warns of Rise of 'Cybertorture' to Bypass Physical Ban*, THE GUARDIAN (Feb. 21, 2020, 6:32 AM), https://www.theguardian.com/law/2020/feb/21/un-rapporteur-warns-of-rise-of-cybertorture-to-bypass-physical-ban.

[279] *See id.*

[280] Rome Statute, *supra* note 16, art. 7(2)(g).

have considered rights enumerated in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the International Covenant on Economic, Social and Cultural Rights when determining whether or not fundamental rights have been violated.[281] The Council of Advisers considered that in a cyber context, if courts would recognize the right of privacy as a fundamental right protected from persecution, this would significantly broaden the court's potential purview over cyber operations. According to Article 7(1)(h), persecution is a discriminatory act, requiring the accused to have targeted civilians "by reason of the identity of a group or collectivity or targeted the group or collectivity as such"[282] based on "political, racial, national, ethnic, cultural, religious, gender as defined in paragraph 3, or other grounds that are universally recognized as impermissible under international law, in connection with any act referred to in this paragraph or any crime within the jurisdiction of the Court."[283] The Council of Advisers considered that China's use of cyber technology in its treatment of the Uyghur Muslim population may be considered persecution under Article 7(1)(h). The current treatment of the Uyghur population in China is facilitated by the use of technology—many detainees are arrested for having allegedly committed religious or political transgressions on social media apps.[284] Collection of this information is possible because Uyghurs are required to present their smartphones at checkpoints around Xinjiang Autonomous Region.[285] Meanwhile, AI, facial recognition, and other software is used to monitor movement of the population and scan online communications for religious speech.[286] The Council of Advisers agreed that this is an example of the ways that cyber technology could be used to facilitate persecution of a group on what appear to be prohibited grounds, assuming that all the contextual elements for crimes against humanity are also met. The Council of Advisers also noted that the Rome Statute uniquely requires that persecution take place, "in connection with any act referred to in [Article 7(1)] or

---

[281] *See* WILLIAM A. SCHABAS, GENOCIDE IN INTERNATIONAL LAW 195–96 (2d ed. 2009).
[282] *See* Elements of Crimes, *supra* note 70, at art. 7(1)(h), ¶ 2.
[283] Rome Statute, *supra* note 16, art. 7(1)(h).
[284] Darren Byler, *China's Hi-Tech War on Its Muslim Minority*, THE GUARDIAN (Apr. 11 2019), https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-recognition.
[285] *See id.*
[286] *See id.*

any crime within the jurisdiction of the Court."[287] It is not entirely clear what kind of connection would be required, and the ICC has yet to interpret this requirement in a meaningful way.[288] The Council of Advisers did not, however, believe that this requirement would be a significant barrier to considerations of cyber operations as crimes against humanity under Article 7(1)(h).

17. Although inhumane acts under Article 7(1)(k) have not been exhaustively defined,[289] the Council of Advisers considered that cyber operations resulting in "great suffering, or serious injury to body or to mental or physical health"[290] that do not fall into one of the other enumerated acts could be prosecuted by the ICC as an inhumane act. The ICC requirements are similar to the jurisprudence of the ad hoc tribunals which would require acts of similar gravity and seriousness to that of other prohibited acts.[291]

SECTION IV: CONCLUSION

18. Based on their discussions, the Council of Advisers concluded that cyber operations could potentially satisfy each of the contextual elements required by the Rome Statute to constitute crimes against humanity under Article 7. However, there remain several challenges and open questions based on the nature of cyber operations, some that are relevant to each of the Rome Statute's enumerated crimes, and others particular to Article 7.

19. One of the points of disagreement in the discussion, as summarized above, is how the court will look at exclusively non-physical effects of cyber operations. Though as discussed, cyber operations can be used to engage in physical violence against a civilian population, it might be more likely for the harm caused by a cyber operation to be psychological or non-physical. Including exclusively psychological or mental harm under crimes

---

[287] Rome Statute, *supra* note 16, art. 7(1)(h). *C.f.* Prosecutor v. Kupreskic, Case No. IT-95-16-T, Judgment, ¶ 580 (Int'l Crim. Trib. for the Former Yugoslavia Jan. 14, 2000) (finding that the definition of persecution in Article 7(1)(h) requiring persecution to be charged in connection with another crime under the Statute is "not consonant with customary international law.").

[288] *See* METTRAUX, *supra* note 267, at 673–75.

[289] *See* SCHABAS, *supra* note 64, at 206–09.

[290] Rome Statute, *supra* note 16, art. 7(1)(k).

[291] *See* Elements of Crimes, *supra* note 70, at Art. 7(1)(k) ¶ 2.

against humanity would have meaningful ramifications for the future of cyber operations. Based on the definition of several enumerated crimes, as noted by members of the Council of Advisers, the drafters of the Rome Statute specifically included mental harm and other non-physically violent crimes under crimes against humanity (and other crimes within the jurisdiction of the ICC), which dictates that cyber operations with exclusively psychological effects could come before the court.[292] Because the ICC and ad hoc tribunals have only had occasion to address crimes that have produced either exclusively physical harms or both physical and mental harm, it remains unclear how the ICC would address conduct that caused exclusively non-physical suffering. An additional complicating factor is that such conduct would first have to meet the ICC's gravity threshold for admissibility.

20. As stated in Section II above, in the context of cyber operations, the contextual element of knowledge may be more difficult to establish. This is in large part because attribution of cyber acts to a particular State or group is notoriously difficult.[293] As noted in the next chapter on the Crime of Genocide, States may attempt to disguise their cyber activity[294] or may outsource cyber activity to "black-hat" hackers, who can be difficult to individually trace[295] and even more difficult to link back to State officials giving orders.[296] Some cyber operations may have several actors.[297] If such cyber activity is outsourced, it may be more difficult to establish that the perpetrators of a particular attack had knowledge of a broader widespread or systematic attack against a civilian population or that their conduct was part of a State or organizational plan or policy. As noted by the Council of Advisers, knowledge can often be inferred from the circumstances. In other words, circumstances can support the idea that it is unlikely that the perpetrator would not know they were participating in a broader attack.

---

[292] Emerging concepts like cyber torture suggest that jurisprudence could move in this direction. *See* Bowcott, *supra* note 278.

[293] The Council of Advisers focused on individual criminal responsibility and mainly set aside the questions of State responsibility.

[294] Reports emerged in October 2019 that Russian hackers had latched on to an Iranian cyber operation and were able to attack organizations in several countries, while disguised as Iranian actors. *See* Stubbs & Bing, *supra* note 94.

[295] *See* Chaumette, *supra* note 90, at 24–25.

[296] *See id.* at 25.

[297] *See id.*

However, this conception is challenging in the context of cyber operations, among others, where operatives may be launching attacks from anywhere in the world.

21. The challenges of attribution as well as of proving intent also introduce complications for establishing the nexus between the individual act and the underlying attack required to establish a crime against humanity under Article 7 of the Rome Statute. As noted in Section II above, in the case of a cyber operation, the ICC would consider "the characteristics, the aims, the nature or consequences of the [enumerated] act"[298] of which it forms a part. Difficulties of attribution may undermine the perceived nexus between an individual cyber operation and the broader underlying attack. Furthermore, cyber operations often use malware that may act unpredictably either because the perpetrators lack knowledge about a particular system being targeted or because of technical errors.[299] This may lead to unintentional consequences, which means that even if a civilian population suffers a cyber operation, it may be difficult to discern if such a population was the intended target, and therefore whether there is a nexus between the cyber operation and the broader attack. It may be difficult to bring such a situation within the "intent or knowledge" requirement of Article 30 of the Statute.

22. As technology continues to advance and cyber operations become an increasingly important tool for both State and organizational actors, the ICC will likely have occasion to address some of the questions raised and to give clarity on application of Rome Statute Article 7 on crimes against humanity in the context of cyberwarfare.

---

[298] *Bemba* Decision, *supra* note 86, ¶ 86.
[299] *See* Roscini, *supra* note 271, at 266.

PART IV

The Application of Article 6 (Genocide) of the Rome Statute to Cyberwarfare

PART IV: THE APPLICATION OF ARTICLE 6 (GENOCIDE) OF THE ROME STATUTE TO CYBERWARFARE[300*]

SECTION I

The Crime of Genocide in the International Criminal Court: General Overview

The Crime of Genocide is set out in Article 6 of the Rome Statute.[301] The contents of Article 6 were taken directly from Article II of the Convention on the Prevention and Punishment of the Crime of Genocide ("Genocide Convention"), a move that was agreed upon relatively quickly during the drafting of the Statute.[302] The Statutes of the ad hoc tribunals, the International Criminal Tribunal for the Former Yugoslavia (ICTY) and the International Criminal Tribunal for Rwanda (ICTR), also incorporated Article III of the Convention that lists punishable acts of genocide as genocide itself, conspiracy to commit genocide[303], direct and public incitement to genocide, attempt to commit genocide, and complicity in genocide.[304] Notably, the ICC is yet to complete the prosecution of an individual for the crime of genocide, but the court expressed some views on the topic in *Prosecutor v. Bashir*.[305] Given the limited ICC jurisprudence, the Council of Advisers, for the purposes of

---

[300] Dr. Claus Kreß did not participate in the discussions on the application of genocide to cyberwarfare because of a parallel position he had as an ad hoc judge in the case of The Gambia v. Myanmar at the International Court of Justice.

[301] *See* Rome Statute *supra* note 16, art. 6.

[302] GIDEON BOAS, JAMES L. BISCHOFF, & NATALIE L. REID, ELEMENTS OF CRIMES OF UNDER INTERNATIONAL LAW 198 (2008). This is likely because by the time of the drafting, the definition of genocide as established in the Convention reflected customary international law and would be widely accepted by states. *See id.*

[303] It is important to note that conspiracy to commit genocide, while in the ICTY and ICTR Statutes, is not in the Rome Statute.

[304] *See* BOAS, BISCHOFF & REID, *supra* note 302, at 199.

[305] *See* Claus Kreß, *The ICC's First Encounter with the Crime of Genocide: The Case against Al Bashir*, *in* THE LAW AND PRACTICE OF THE INTERNATIONAL CRIMINAL COURT 669, 669–70 (Carsten Stahn ed., 2015). Former President of Sudan, Omar al-Bashir has been charged with genocide. *See id.* The Pre-Trial Chamber expressed some views on the crime in its 2009 and 2010 Decisions on the Prosecution's Application for a Warrant of Arrest.

this report, also looked to the ad hoc tribunals for guidance on how the ICC might interpret the crime of genocide.

Article 9 of the Rome Statute points the court to the Elements of Crimes, an instrument meant to assist the court in interpreting Articles 6, 7, 8 and 8*bis*.[306] Although the Elements which are adopted by the States Parties are only binding on the ICC, they offered non-binding guidance for the ad hoc international tribunals which often considered them as persuasive guidance.[307] The ICC *Bashir* Pre-Trial Chamber referred to the Elements numerous times in its interpretation of genocide.[308]

The Mental Element: Specific Intent

According to the ICC *Bashir* Pre-Trial Chamber, there are two mental elements in the crime of genocide: the general requirements laid out in Article 30 of the Rome Statute—intent and knowledge—and the additional intent specific to genocide, the *dolus specialis*.[309] This *dolus specialis* is enumerated in the chapeau of Article 6: acts of genocide must be "committed with intent to destroy, in whole or in part, a national, ethnical, racial or religious group, as such."[310] Such intent need not necessarily be proven directly, but may be inferred from the circumstances and facts of a particular case.[311] Further, assessment of intent should be considered not only in light of the particular conduct of the accused, but in light of all conduct of those participating.[312]

---

[306] *See* BOAS, BISCHOFF & REID, *supra* note 302, at 201. *See also* Elements of Crimes, *supra* note 70, at 5, ¶ 2.

[307] Leanne McKay, *Characterising the System of the International Criminal Court: An Exploration of the Role of the Court Through the Elements of Crimes and the Crime of Genocide,* 6 INT'L CRIM. L. REV. 257, 267 (2006).

[308] Prosecutor v. Bashir, ICC-02/05-01/09-94, Second Decision on the Prosecution's Application for a Warrant of Arrest, ¶ 8, 13, 20, 26, 33 (July 12, 2010) [hereinafter Bashir 2010 Decision].

[309] Bashir 2009 Decision, *supra* note 255, ¶ 139.

[310] Rome Statute, *supra* note 16, art. 6.

[311] *See* BOAS, BISCHOFF & REID, *supra* note 302, at 160; *see also* SCHABAS, *supra* note 281, at 265. Tribunals have considered systematic targeting of a particular group, the scale of atrocities committed against that group, the number of members affected, derogatory language used toward the group, and other conduct that might not itself qualify as genocide but that aims at the foundation of the group, as circumstantial evidence for genocidal intent. *See* BOAS, BISCHOFF & REID, *supra* note 302, at 160–61.

[312] *See* BOAS, BISCHOFF & REID, *supra* note 302, at 164.

Of particular importance are interpretations of the word "destroy" and the phrase, "in whole or in part." The ILC, along with ad hoc tribunal jurisprudence, have interpreted "destroy" to mean exclusively physical or biological destruction and not the national, religious, cultural, or linguistic destruction of a particular group.[313] During the drafting of the Genocide Convention, after much discussion, the parties deliberately excluded cultural genocide from the Convention.[314] Additionally, neither the ILC nor the drafters of the Rome Statute decided to add cultural genocide to the definition of the crime of genocide.[315] Intent of cultural or social destruction, however, could be used as evidence toward establishing genocidal intent.[316] The *Bashir* Pre-Trial Chamber appeared to follow the standard set by prior case law, emphasizing the physical destruction of the group, as opposed to its mere dissolution.[317]

The ad hoc tribunals have considered that conduct will only qualify as genocide if the portion of the group targeted is significant enough to impact the group as a whole.[318] Importantly, though, even one victim is enough to satisfy the material element of the crime, as long as the accused exhibited an intent to destroy a part or the whole of a particular group.[319] The *Bashir* Pre-Trial Chamber appeared to adopt the now-accepted view that "part" of a group must be substantial, but substantiality may be assessed either quantitatively or qualitatively.[320] A quantitative assessment considers the absolute number of individuals targeted, as well as that number's relation to the overall size of the entire group, while a qualitative assessment may consider if the part is prominent within the group, emblematic of the

---

[313] *See* BOAS, BISCHOFF & REID, *supra* note 302, at 164-65. The International Court of Justice has also affirmed physical destruction as the meaning of "destroy." Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, 2007 I.C.J. 43, ¶ 344 (Feb. 26); Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Croatia v. Serbia), Judgment, 2015 I.C.J. 3, ¶ 136 (Feb. 3).

[314] *See* SCHABAS, *supra* note 281, at 213. Many drafting delegates considered cultural genocide a human rights issue rather than an international criminal one. *See id.*

[315] *See id* at 220.

[316] *See* BOAS, BISCHOFF & REID, *supra* note 302, at 165; *see also* SCHABAS, *supra* note 281, at 271–72.

[317] *See* Kreß, *supra* note 305, at 692.

[318] *See* BOAS, BISCHOFF & REID, *supra* note 302, at 168.

[319] *See* SCHABAS, *supra* note 281, at 276.

[320] *See* Kreß, *supra* note 305, at 692.

group, or essential to its survival.[321]

The Elements of Crimes of the ICC lays out an additional common element for each act of genocide, requiring that, "[t]he conduct took place in the context of a manifest pattern of similar conduct directed against that group or was conduct that could itself effect such destruction."[322] This contextual element was meant to prevent trivialization of the scale or threat to a group required for a crime to constitute genocide and to exclude isolated hate crimes from consideration under Article 6.[323] The resulting language appears to cautiously support the idea that the crime of genocide requires a plan or policy ("manifest pattern of similar conduct"). Although the ad hoc tribunals have not considered a plan to be a specific legal ingredient for the crime of genocide,[324] it is difficult to imagine genocide without some systematic policy, preparation or planning.[325]

The *Bashir* Pre-Trial Chamber acknowledged that recognition of the contextual element in the Elements of Crimes remains controversial but interpreted the requirement of a "context of a manifest pattern" to indicate that "the crime of genocide is only completed when the relevant conduct presents a concrete threat to the existence of the targeted group, or a part thereof,"[326] and that the threat must be "concrete and real, as opposed to just being latent or hypothetical."[327] This interpretation, which marks a departure from the ICTY approach, seems to support efforts to prevent the trivialization of the crime of genocide.

The *Bashir* Pre-Trial Chamber also observed that an act of genocide, must satisfy—in addition to specific intent (*dolus specialis*)—the general subjective elements of intent and knowledge as laid out in Article 30 of the Rome Statute.[328] There remains some disagreement within the ICC regarding the degree of knowledge or intent required to satisfy the

---

[321] Bashir 2009 Decision, *supra* note 255, ¶ 146.

[322] Elements of Crimes, *supra* note 70, at Article 6(a), ¶ 4. This contextual element is listed as the final element for each of act of genocide, Article 6(a)–(e). *Id.* at 6-8.

[323] *See* McKay, *supra* note 307, at 263; *see also* BOAS, BISCHOFF & REID, *supra* note 302, at 202.

[324] *See* SCHABAS, *supra* note 281, at 244–45; *see* McKay, *supra* note 307, at 265.

[325] *See* SCHABAS, *supra* note 281, at 267; *see also* McKay, *supra* note 307, at 264–65. Proof of a plan or inference that one exists will "inevitably be an important element in the prosecution case." SCHABAS, *supra* note 281, at 267.

[326] Bashir 2009 Decision, *supra* note 255, at ¶ 124.

[327] *See id.* A member of the Council believes that the concrete threat requirement could be interpreted in a matter which is too restrictive.

[328] Bashir 2009 Decision, *supra* note 255, at ¶ 139.

requirements of Article 30. In particular, unintended but foreseeable consequences are most likely simply not covered, and certainly unforeseeable ones are not covered.[329] While this question is not completely resolved, given the high threshold for the *dolus specialis* of the crime of genocide, and the emphasis on the purposeful nature of genocidal acts, it is unlikely that foreseeable but unintended consequences would satisfy the threshold and thereby produce criminal responsibility in a genocide context.[330]

SECTION II

The following section reflects the Council of Advisers' exchange on whether cyber operations may constitute the crime of genocide as enumerated in Article 6 of the Rome Statute. For the purposes of this chapter, a "targeted group" is any national, ethnic, racial or religious group whose members are attacked on the basis of their membership in the group.

---

[329] Mohamed Elewa Badar & Sara Porro, *Article 30, Mental Element*, *in* COMMENTARY ON THE LAW OF THE INTERNATIONAL CRIMINAL COURT 314, 316–19 (Mark Klamberg ed., 2017). Some ICC jurisprudence and scholarship suggest that *dolus eventualis*, or recklessness might be read into Article 30, which would cover conscious risk-taking or foreseeable consequences, even if those consequences were not the intended goal of a perpetrator. *See id.* at 317. More recent jurisprudence, particularly, *Prosecutor v. Bemba,* argued that this lower level of culpability could not be read into the statute because Article 30 requires that a perpetrator is aware that a consequence "*will* occur in the ordinary course of events," thereby requiring close to certainty. *See id.* at 318 (emphasis added); *Bemba* Decision, *supra* note 86, ¶ 362-63.

[330] Roberta Arnold, *The Mens Rea of Genocide Under the Statute of the International Criminal Court,* 14 CRIM. L. F. 127, 140 (2003). The 1996 Draft Code of Crimes against the Peace and Security of Mankind specifically argued that mere awareness of probable consequences of one of the enumerated acts is insufficient to constitute genocide and that the crime requires a specific state of mind and intent regarding the consequences of a genocidal act. *See id.* Additionally, the drafters of the Elements of Crimes considered including language typically associated with negligence, namely, that an accused "knew or should have known that the conduct would destroy, in whole or in part. . . ," but such language was rejected. *See* SCHABAS, *supra* note 281, at 254-55. For the argument that recklessness, dolus eventualis and negligence are excluded by the language and preparatory work of the Statute, *see* Roger S. Clark, *The Mental Element in International Criminal Law: The Rome Statute of the International Criminal Court and the Elements of Offences*, 12 CRIM. L. F. 291, 300-01 (2001); Roger S Clark, *Drafting a General Part to a Penal Code: Some Thoughts Inspired by the Negotiations on the Rome Statute of the International Criminal Court and by the Court's First Substantive Law Discussion in the Lubanga Dyilo Confirmation Proceedings*, 19 CRIM. L. F. 519, 525 (2008).

Article 6(a) Killing Members of the Group

A cyber operation satisfying the requisite mental elements would constitute the crime of genocide if such an operation attempted to cause or caused the death of members of a targeted group, in whole or in substantial part.

1. The Elements of Crimes state that the term "killed" is interchangeable with the term "caused death."[331] Additionally, what differentiates killing as an act of genocide from murder under crimes against humanity is that genocidal killings "must be directed against members of a national, ethnical, racial or religious group."[332] Assuming the *dolus specialis* is met, the Council of Advisers agreed that cyber means could be used to carry out an act of genocide under Article 6(a). Cyber operations may be used, for example, to shut down the cooling system in a nuclear power plant, causing the release of radioactive materials and resulting in the death of civilians living near the plant.[333] This could be considered an act of genocide under Article 6(a) if the civilians targeted were members of a national ethnic, racial or religious group and they were targeted with the intent to destroy, in whole or in part, the group. Similarly, a cyber operation on a dam or water network leading to floods that kill members of another national, ethnic, racial or religious group based on their membership in that group, or a cyber operation that disrupts air traffic control systems leading to the deaths of members of a such targeted group on a downed plane could also constitute the crime of genocide under Article 6(a) if accompanied by intent to destroy the group or a substantial part of the group.[334] As noted earlier, the above conduct must either take place in the context of the manifest pattern of similar conduct directed against that group, or be conduct that could itself effect such destruction. It would appear that cyber operations combined with other types of physical

---

[331] Elements of Crimes, *supra* note 70, at art. 6(a) ¶ 1, n.2. There was a jurisprudential debate on the term "killing" between the *Akayesu* and *Kayishema* Chambers at the ICTR. "Killing" in English does not indicate intention or whether recklessness in causing death is sufficient. In the former case, the Trial Chamber found "killing" too general. In the latter, the French term "*meurtre*" was said to be more precise, although the Chamber found the two terms equivalent vis-à-vis their use in the Genocide Convention. Prosecutor v. Kayishema, Case No. ICTR-95-1-A, Judgment, ¶ 150–51 (Dec. 4, 2001).

[332] Bashir 2010 Decision, *supra* note 308, at ¶ 20.

[333] See Roscini, *supra* note 271, at 250.

[334] *See id.* at 261.

attacks would be sufficient to meet either of these two conditions since the purpose of the conduct element does not require that the crime take place in a specific physical or electronic domain.

Article 6(b) Causing Serious Bodily or Mental Harm to Members of the Group

A cyber operation satisfying the requisite mental elements would constitute the crime of genocide if such an operation attempted to cause or caused serious bodily harm to members of a protected group, in whole or in substantial part. A cyber operation attempting to cause or causing exclusively serious *mental* harm would constitute the crime of genocide if such an operation took place in the context of other conduct from which a tribunal could infer intent to physically or biologically destroy a protected group, in whole or in substantial part.

2. Serious bodily or mental harm is a uniquely broad category which covers a potentially wide range of conduct. The ad hoc tribunals have referred to serious bodily harm as "harm that seriously injures the health, causes disfigurement or causes any serious injury to the external [or] internal organs or senses."[335] Case law has also established that serious bodily or mental harm must cause "a grave and long-term disadvantage to a person's ability to lead a normal and constructive life."[336] The ICTR's *Akayesu* Trial Chamber described serious bodily or mental harm as "acts of torture, be they bodily or mental, inhumane or degrading treatment, [or] persecution."[337] The Elements of Crimes of the Rome Statute further note that serious bodily and mental harm "may include, but is not necessarily restricted to, acts of torture, rape, sexual violence or inhuman or degrading treatment."[338] Rules of evidence of the ad hoc tribunals have established

---

[335] *See* SCHABAS, *supra* note 281, at 182.

[336] *See* Kreß, *supra* note 305, at 687 (citing Prosecutor v. Krstić, Case No. IT-98-33-T, Judgment, ¶ 513 (Int'l Crim. Trib. for the Former Yugoslavia Aug. 2, 2001)).

[337] Prosecutor v. Akayesu, Case No. ICTR-96-4-T, Judgment, ¶ 504 (Sept. 2, 1998).

[338] Elements of Crimes, *supra* note 70, at art. 6(b) ¶ 1, n.3. The *Akayesu* Trial Chamber first established that rape and sexual violence may constitute genocide under serious bodily and mental harm. *See* SCHABAS, *supra* note 281, at 183.

that serious bodily or mental harm requires proof of a result, which is evaluated by assessing not only specific acts, but a totality of the circumstances surrounding those acts, along with an assessment of a direct or proximate causal link between the accused's acts and the resulting harms.[339] The Council of Advisers agreed that, similar to Article 6(a), a cyber operation meeting the requisite *mens rea* and resulting in serious bodily harm of members of a targeted group, that falls within a protected category, could constitute the crime of genocide.

3. While bodily harm is more straightforward, a clear definition of mental harm remains elusive, as does the value-laden term of "serious." The ad hoc tribunals have maintained that mental harm should be interpreted on a case-by-case basis.[340] Importantly, mental harm need not manifest physically,[341] nor must it be "permanent or irremediable."[342] However, it has been "understood to mean more than the minor or temporary impairment of mental faculties."[343]

4. There is limited jurisprudence on conduct that falls under the category of mental harm. The ICTY in *Prosecutor v. Blagojević*, found that "[t]he fear of being captured, and, at the moment of the separation, the sense of utter helplessness and extreme fear for their family and friends' safety as well as for their own safety, is a traumatic experience from which one will not quickly – if ever – recover,"[344] and "the men [at Srebrenica] suffered mental harm having their identification documents taken away from them, seeing that they would not be exchanged as previously told, and when they understood what their ultimate fate was."[345] Tribunals have further recognized that acts causing mental harm "include threats of death and

---

[339] *See* Nema Milaninia, *Understanding Serious Bodily or Mental Harm as an Act of Genocide*, 51 VAND. J. OF TRANSNAT'L L. 1381, 1396–98 (2018).
[340] *See* BOAS, BISCHOFF & REID, *supra* note 302, at 181; *see also* Milaninia, *supra* note 339, at 1387.
[341] *See* Milaninia, *supra* note 339, at 1393.
[342] *Id.* at 1394 (citing Prosecutor v. Krstić, Case No. IT-98-33-T, Judgment, ¶ 510 (Int'l Crim. Trib. for the Former Yugoslavia Aug. 2, 2001)).
[343] *Id.* (citing Rep. of the Preparatory Comm. on the Establishment of an Int'l Criminal Court, at 11, n.3, U.N. Doc. A/CONF.183/Add.1, at 11 n.3 (Apr. 14, 1998)).
[344] *See* SCHABAS, *supra* note 281, at 185 (citing Prosecutor v. Blagojević, Case No. IT-02-60-T, Judgment, ¶ 647 (Int'l Crim. Trib. for the Former Yugoslavia Jan. 17, 2005)).
[345] *Id.*

knowledge of impending death; acts causing intense fear or terror; surviving killing operations; forcible displacement; and 'mental torture.'"[346] The Council of Advisers noted that serious mental harm is distinct from emotional or psychological damage or attacks on human dignity that do not cause lasting damage.[347] Similarly, a state of anxiety has not been found to be mental harm.[348] The ICC has yet to more seriously engage with this particular act of genocide; jurisprudence has left the list of acts that fall into this category non-exhaustive, and the assessment remains a fact-specific one.[349]

5. Based on the above, with regard to cyber conduct, the Council of Advisers agreed that a cyber operation is just as likely as a kinetic attack to have a mental impact. With limited jurisprudence and interpretation, the non-exhaustive list of conduct that might constitute serious mental harm leaves potential room for cyber operations to qualify as an act of genocide under Article 6(b). Sustained cyber operations could fall into the category of degrading treatment or be used to create fear and terror among a targeted group that—with the appropriate context and *mens rea*—may qualify as an act of genocide.

6. The Council of Advisers discussed a scenario where the use of cyber technologies targeting a certain minority group could amount to genocide in the appropriate circumstances. In the scenario, malicious websites are used to hack into the members of the minority community and malware allows the attackers access to their phones' software, including messages, passwords, and the real-time location of the user. Such sites may be coupled with technological means of surveillance already in place, including cameras equipped with facial and voice recognition and the use of machine algorithms to monitor popular messaging applications and other internet activity for "suspicious" behavior. Using this technology, the State can aggregate data about individuals to create a "predictive policing" program. Such extensive surveillance may produce intense and prolonged fear and anxiety in the population being monitored. Those monitored may fear repercussions for themselves and for their family's safety to an extent that it

---

[346] Milaninia, *supra* note 339, at 1394.
[347] *See id.*
[348] *See id.* at 1395.
[349] *See id.* at 1387.

produces mental harm that inflicts a "grave and long-term disadvantage to a person's ability to lead a normal and constructive life."[350]

7. The Council of Advisers cautioned that currently, cyber operations alone that cause exclusively mental harm would likely not reach the *mens rea* threshold of an act of genocide.[351] This is because, as explained in Section I, the intent to destroy required for genocide is still understood as physical or biological destruction,[352] while intent to cause the cultural dissolution of a group, or cultural genocide, is not recognized as a crime under international law.[353] The Council of Advisers considered that this issue remains somewhat unsettled.[354]

8. The Council of Advisers also considered whether the qualification of cyber operations causing mental harm as an act of genocide under Article 6(b) may also depend on how tribunals interpret the gravity threshold for the *actus reus* of "serious" harm.[355] Though no tribunal has defined the term, the ICTY's Appeals Chamber in *Tolimir* supplied the following:

> [the harm] must be of such a serious nature as to contribute or tend to contribute to the destruction of all or part of the

---

[350] *See* Kreß, *supra* note 305, at 687 (citing Prosecutor v. Krstić, Case No. IT-98-33-T, Judgment, ¶ 513 (Int'l Crim. Trib. for the Former Yugoslavia Aug. 2, 2001)).

[351] Such conduct may also fail to reach the ICC gravity threshold for admissibility, as discussed in Part IV Section II.

[352] *See* BOAS, BISCHOFF & REID, *supra* note 302, at 164-65.

[353] *See* SCHABAS, *supra* note 281, at 220.

[354] *See* Kreß, *supra* note 305, at 692; Judge Shahabuddeen in a partial dissent in *Prosecutor v. Krstić*, proposed a theory by which intent to destroy need not exclusively be physical or biological if it is attached to an enumerated act, which largely involves physical or biological consequences. Importantly, Judge Shahabuddeen specifically stated that this was not an argument for the recognition of cultural genocide, and summarized his contention that "the Statute is to be read to mean that, provided that there is a listed act (this being physical or biological), the intent to destroy the group as a group is capable of being proved by evidence of an intent to cause the non-physical destruction of the group in whole or in part." Prosecutor v. Krstić, Case No. IT-98-33-A, Judgment, Partial Dissent Opinion of Judge Shahabudeen, ¶54 (Int'l Crim. Trib. for the Former Yugoslavia Aug. 2, 2001). The ICTY Trial Chambers in later cases, *Prosecutor v. Blagojević and Jokić* and *Prosecutor v. Krajisnik* adopted Judge Shahabuddeen's arguments, suggesting a move toward an expanded interpretation of "intent to destroy." Prosecutor v. Blagojević, Case No. IT-02-60-T, Judgment, ¶659, (Int'l Crim. Trib. for the Former Yugoslavia Jan 17, 2005); Prosecutor v. Krajišnik, Case No. IT-00-39-T, Judgment, ¶854 (Int'l Crim. Trib. for the Former Yugolsavia Sept. 27, 2006).

[355] "Serious" harm in the context of the ICC would also have to surpass the gravity threshold discussed in Part IV Section II and outlined in Rome Statute Art. 17(1)(d), to be admissible. Rome Statute, *supra* note 16, art. 17 ¶1(d).

> group; although it need not be permanent or irreversible, it must go "beyond temporary unhappiness, embarrassment or humiliation" and inflict "grave and long-term disadvantage to a person's ability to lead a normal and constructive life."[356]

9. Though there is only limited jurisprudence offering meaningful interpretation of the above definition,[357] the idea that an act causing serious bodily or mental harm should "contribute, or tend to contribute, to the destruction of the protected group or part thereof," does have some support in ad hoc tribunal case law[358] and the ICJ.[359] Should the ICC also choose to adopt this aspect of the definition, the Council of Advisers agreed that this would further tend to support the proposition that cyber operations that satisfy the mental elements of genocide, but exclusively cause mental harm, would likely have to take place in the context of conduct that threatens the physical destruction of the targeted protected group, or a substantial part of the targeted protected group, in order to constitute an act of genocide. On its own, the cyber operation may not reach this higher threshold for *actus reus* for genocide, though the Council noted that as technology evolves, this assessment may change.

10. The Council of Advisers assessed that with increasing dependence on technology and its subsequent increased control over day-to-day life, development of cyber tools and weapons may come to shape the way Tribunals and scholars view the concepts of destruction and of mental harm. International legal scholars and practitioners may soon need to consider the ideas of digital destruction of a particular group and forms of cyber torture. In the meantime, however, the Council of Advisers determined that currently, though cyber operations capable of causing mental harm, such as the extensive surveillance and cyber intimidation discussed above, could constitute an act of genocide under Article 6(b), such conduct would likely only be considered genocidal in the context of additional

---

[356] *See* Milaninia, *supra* note 339, at 1402 (citing Prosecutor v. Tolimir, Case No. IT-05-88/2-A, Judgment, ¶¶ 201–02 (Int'l Crim. Trib. for the Former Yugoslavia Apr. 8, 2015).

[357] *See id.* at 1402–04.

[358] *See id.* at 1405 (citing Prosecutor v. Krajišnik, Case No. IT-00-39-T, Judgment, ¶ 861 (Int'l Crim. Trib. for the Former Yugoslavia Sept. 27, 2006)).

[359] *See id.* at 1408 (citing Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Croat. v. Serb.), Judgment, 2015 I.C.J. Rep. 118, ¶ 157 (Feb. 3)). This position was later adopted by the *Tolimer* Tribunal in their Appeal Judgment. *See id.* at 1408.

physically destructive conduct.

Article 6(c) Deliberately Inflicting on the Group Conditions of Life Calculated to Bring About Its Physical Destruction in Whole or in Part

A cyber operation satisfying the requisite mental elements would constitute the crime of genocide if such an operation deliberately inflicted on the group conditions of life calculated to bring about its physical destruction in whole or in part.

11. The ICTR described the expression "deliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part" as "the methods of destruction by which the perpetrator does not immediately kill the members of the group, but which, ultimately, seek their physical destruction."[360] The Elements of Crimes of the ICC state that "'conditions of life' may include, but is not necessarily restricted to, deliberate deprivation of resources indispensable for survival, such as food or medical services, or systematic expulsion from homes."[361] The ad hoc tribunals have also found that "the imposition of a subsistence diet; a forced lack of proper housing, clothing or hygiene; and requiring excessive work or physical exertion,"[362] may qualify as an act of genocide under this provision. The Council of Advisers agreed that a cyber operation could create conditions threatening the survival of a group. For example, cyber operators could disable the power grid for a significant period of time over a severely cold winter[363] or use cyber means to cut off access to medical services by disrupting the networks in

[360] Prosecutor v. Akayesu, Case No. ICTR-96-4-T, Judgment, ¶ 505 (Sept. 2, 1998). Because the act specifies "physical destruction," ethnic cleansing of a territory, which might lead to the dissolution, rather than destruction of a group, does not qualify as an act of genocide. *See* Kreß, *supra* note 305, at 688.

[361] Elements of Crimes, *supra* note 70, at art. 6(c), ¶ 4, n.4.

[362] BOAS, BISCHOFF & REID, *supra* note 302, at 184.

[363] *See* Roscini, *supra* note 271, at 261; Cyber operations targeting a national power grid have already taken place in Ukraine, just before Christmas in 2016. *See* Andy Greenberg, *New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction,* WIRED (Sept. 12, 2019, 11:55 AM), https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/.

local hospitals servicing members of another national, ethnic, racial or religious group.

12. A question arises concerning what is usually referred to as "ethnic cleansing," which, according to the ICJ, can be defined as "rendering an area ethnically homogenous by using force or intimidation to remove persons of given groups from the area."[364] This notion is understood as distinct from genocide. However, the *Al Bashir* Pre-Trial Chamber determined that certain practices, such as "ethnic cleansing," may well amount to genocide if they bring about the commission of the objective elements of genocide provided for in Article 6 of the Rome Statute and the Elements of Crimes with the specific intent to partly or wholly destroy the targeted group.[365] Setting aside the "force" element, and focusing on the "intimidation" aspect in the ICJ's definition, it might be possible in a cyber operations context to envisage a deliberate targeting of a group through a disinformation campaign that targets a protected group with a "calculated" purpose to intimidate and bring about more than the departure of members of the group, to accomplish destruction of the group in whole or in part. Where there are parallel acts by those carrying out physical/kinetic attacks and those carrying out the cyber operations, it would be even harder to argue that genocide has not occurred assuming the presence of specific intent.

Article 6(d) Imposing Measures Intended to Prevent Births within the Group

A cyber operation satisfying the requisite mental elements would constitute the crime of genocide if such an operation was designed with the intention of reducing or preventing pro-creation within a targeted protected group.

13. The ICTR *Akayesu* Trial Chamber considered conduct that would qualify as directly intended to prevent births to include sexual mutilation, sterilization, forced birth control, and prohibition of marriages.[366] Births may

[364] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, 2007 I.C.J. 43, ¶ 190 (Feb. 26).
[365] Bashir 2009 Decision, *supra* note 255, ¶ 143-45.
[366] *See* Prosecutor v. Akayesu, Case No. ICTR-96-4-T, Judgment, ¶ 507 (Sept. 2, 1998).

also be prevented by indirect mental means, such as rape or other trauma that would lead individuals to refuse to procreate.[367] The Council of Advisers agreed that a cyber operation could possibly constitute such a measure. Though not direct, the Council discussed the possibility that an actor could launch a disinformation campaign designed to dissuade or forbid members of another national, ethnic, racial or religious group from procreating. The Council further suggested that an actor could specifically alter online medical records of members of the targeted group, which could lead those individuals to refrain from procreating by, for example, falsifying genetic markers for serious birth defects, leading to termination of pregnancies.

Article 6(e) Forcibly Transferring Children of the Group to Another Group

A cyber operation satisfying the requisite mental elements would constitute the crime of genocide if such an operation intended to force members of a group to transfer their children to another group.

14. The Elements of Crimes of the ICC specify that "'forcibly' is not restricted to physical force, but may include threat of force or coercion, such as that caused by fear of violence, duress, detention, psychological oppression or abuse of power, against such person or persons or another person, or by taking advantage of a coercive environment."[368] The Council of Advisers agreed that cyber operations could be used to create psychological oppression by way of systematic dissemination of threatening information over social media platforms or by State surveillance of another national, ethnic, racial or religious group that would compel members of the group to transfer their children to another group. Cyber technology could also be used in policies of taking children into care and then losing or otherwise prohibiting access to the digital records, making the children's details inaccessible to the parents.

---

[367] *See id.* ¶ 508.

[368] Elements of Crimes, *supra* note 70, at art. 6(e), ¶ 1, n.5.

SECTION III

The following section reflects the Council of Advisers' exchange regarding direct and public incitement to genocide using cyber operations.

Article 25(3)(e) In respect of the Crime of Genocide, Directly and Publicly Incites Others to Commit Genocide

Cyber operations may be employed to carry out the crime of direct and public incitement to genocide.

15. Article 25(3)(e) creates criminal responsibility for an individual who "directly and publicly incites others to commit genocide."[369] "Public" requires a "call for criminal action to a number of individuals in a public place or to members of the general public at large"[370] and can be communicated via mass media such as radio or television.[371] The Council of Advisers noted that cyberspace, namely, the Internet, would easily satisfy the criteria for a space where public incitement to genocide could take place.[372] Direct incitement merely requires that the content of the incitement be specific, as to explicitly provoke others to commit acts of genocide against a targeted group.[373] Importantly, jurisprudence, particularly the ICTR *Akayesu* Trial Chamber, has recognized that incitement to genocide may be communicated through euphemisms and that language should be assessed based on cultural and linguistic context.[374] The Council of Advisers considered this very relevant for incitement to genocide in a cyber context. Furthermore, incitement to genocide must be distinguished from hate speech and other incitement to violence, though incitement to genocide will also often be accompanied by various forms of hate speech.[375] Some hate speech and incitement to violence will be discriminatory in nature and be violative of human rights law, without necessarily rising to conduct that is genocidal

---

[369] Rome Statute, *supra* note 16, art. 25(3)(e).
[370] SCHABAS, *supra* note 281, at 329. *See also* Chaumette, *supra* note 90, at 32.
[371] *See* Chaumette, *supra* note 90, at 32.
[372] *See id.*
[373] *See id.* at 33.
[374] *See* Prosecutor v. Akayesu, Case No. ICTR-96-4-T, Judgment, ¶ 557 (Sept. 2, 1998).
[375] *See* SCHABAS, *supra* note 281, at 330.

in nature.[376] An individual accused of direct and public incitement to genocide must share the requisite *dolus specialis* for genocide.

16. While this issue has not yet been addressed by the ICC, the ICTR found inciters responsible for both the crime of direct and public incitement to genocide[377] and the crime of genocide itself,[378] holding that "the killing of Tutsi civilians can be said to have resulted, at least in part, from the message of ethnic targeting for death that was clearly and effectively disseminated through RTLM [radio]."[379] Under the Rome Statute, there has been some debate on whether direct and public incitement to genocide was preserved as an inchoate crime, as in the Genocide Convention, or if it serves only as an additional mode of responsibility for complicity in genocide.[380] Drafting history and commentary, however, suggests that Article 25(3)(e) meant for incitement to remain an inchoate crime,[381] while incitement as complicity is covered under the terms "solicit" and "induce" in Article 25(3)(b).[382] Importantly, the Council of Advisers noted that incitement, as an inchoate crime, must still meet the ICC's gravity threshold, as discussed in Part IV Section II.

17. The Council of Advisers discussed the ways that cyberspace lends itself particularly well to public and direct incitement of genocide. A State actor or private group could launch a powerful disinformation campaign targeting a particular group, inciting first hatred toward the group, and then violence with an intent to destroy. This might look similar to Joseph

---

[376] *See* Kai Ambos, *Individual Criminal Responsibility*, *in* TRIFFTERER & AMBOS, *supra* note 204, at 979, 1018.

[377] *See* Prosecutor v. Nahimana et. al., Case No. ICTR-99-52-T, Judgment and Sentence, ¶¶ 1033-35, 1038-39 (Dec. 3, 2003).

[378] *See id.* at ¶¶ 974-77A.

[379] *See id.* at ¶ 953.

[380] However, it has been argued that the placement of the act in Article 25 limits incitement to a mode of liability, meaning that one can only be responsible for incitement to genocide if a genocide, in fact, occurs or is attempted. *See* Thomas E. Davies, *How the Rome Statute Weakens the International Prohibition on Incitement to Genocide*, 22 HARV. HUM RTS. J. 245, 245 (2009). Some scholars consider that direct and public incitement to genocide in Article 25 remains an inchoate crime, meaning an individual can be liable even if the incitement is unsuccessful and the genocide does not occur or is not attempted. *See* Ambos, *supra* note 372, at 1017. *See also* BOAS, BISCHOFF & REID, *supra* note 302, at 200.

[381] *See* Tahlia Petrosian, *Secondary Forms of Genocide and Command Responsibility under the Statutes of the ICTY, ICTR and ICC*, 17 AUSTL. INT'L L. J. 29, 44 (2010).

[382] *See* TRIFFTERER & AMBOS, *supra* note 204, at 1016.

Goebbels's wide-reaching Nazi propaganda machine or radio stations during the Rwandan genocide, but with access to the broad platform that the internet and social media provide. The Council of Advisers noted how social media has already been used as a platform to incite and spread hatred and violence. For example, the military in Myanmar has been accused of inciting genocide against the country's Rohingya minority via a campaign on Facebook involving hundreds of military personnel.[383] The Council of Advisers concluded that, though cyber technology may be employed to carry out various different acts of genocide with varying modes of responsibility, incitement to genocide by cyber technologies may already be happening and is likely to remain one of the more prolific cyber activities in relation to the crime.

SECTION IV: CONCLUSION

18. With regard to the application of Article 6 to cyber operations, the most glaring open question touched upon by the Council of Advisers is that of Article 6(b) and serious mental harm. This question is crucial because though it was determined by the Council of Advisers that cyber operations may have physical effects that constitute the crime of genocide, cyber operations could also cause psychological harm. Because there is so little jurisprudence interpreting serious mental harm and because international criminal bodies have never had occasion to assess mental harm independent of the physical ones typically associated with genocide,[384] it remains difficult to predict how the ICC would treat such cyber conduct. Notwithstanding the prevailing view that fulfilment of the specific intent requirement for genocide requires physical or biological destruction, the Council of Advisers noted that such physical requirements have been and continue to be challenged in international legal circles. In a recent example—as already mentioned above in the context of discerning a crime against humanity—Nils Melzer, the UN's special rapporteur on torture and other cruel, inhuman or degrading treatment or punishment made

[383] Paul Mozur, *A Genocide Incited on Facebook, with Posts from Myanmar's Military*, N.Y. TIMES (Oct. 15, 2018), https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.

[384] *See* Milaninia, *supra* note 339, at 1394.

clear that torture is not something solely physical.[385] Indeed, the definition of torture in the Convention against Torture makes clear that torture inflicts "severe pain or suffering, whether physical *or mental*."[386] Melzer specifically cited the concept of cyber torture, which, similar to some of the conduct discussed by the Council of Advisers, could "expose targeted individuals to extremely elevated and prolonged levels of anxiety, stress, social isolation and depression, and significantly increases the risk of suicide."[387] The key questions remain whether this conduct along with the intent to cause the physical destruction of the group could constitute the crime of genocide and if it would meet the ICC's gravity threshold for admissibility. The Council of Advisers further noted in their discussion that movement toward a broader interpretation of psychological harms could have significant ramifications for application of the Rome Statute in cyberwarfare across the different enumerated crimes. Moreover, cyber tools or operations may both aid and complicate assessments of genocidal intent. Even if a cyber operation on its own does not meet the threshold for an act of genocide or fall within the category of acts establishing accessory responsibility to genocide, tribunals can look to cyber operations, such as the population-controlling surveillance measures discussed above, as evidence tending to suggest genocidal intent. Because intent may be inferred, cyber operations may be considered as part of the context of a manifest pattern of conduct aimed at the destruction of a group. On the other hand, in the event of a particular cyber operation that may itself qualify as an act of genocide, it may be difficult to discern the particular intent of the users of software used to carry out the operation. The Council of Advisers agreed that these questions would likely be addressed on a case-by-case analysis.

---

[385] *See* Bowcott, *supra* note 278.
[386] *See* Convention against Torture, *supra* note 268.
[387] *See* Bowcott, *supra* note 278.

For feedback and questions please contact newyork@llv.li.