INTERNATIONAL LAW STUDIES

Published Since 1895

Cyber Peacekeeping Operations and the Regulation of the Use of Lethal Force

Nicholas Tsagourias and Giacomo Biggio

99 INT'L L. STUD. 37 (2022)

Volume 99

2022

Published by the Stockton Center for International Law

ISSN 2375-2831

Cyber Peacekeeping Operations and the Regulation of the Use of Lethal Force

Nicholas Tsagourias and Giacomo Biggio***

CONTENTS

* Professor of International Law at the University of Sheffield.

** Teaching Associate at the University of Bristol.

The authors would like to thank Andrea Harrison, Head of Cooperation, International Committee of the Red Cross, for her comments on a previous draft.

The thoughts and opinions expressed are those of the authors and not necessarily those of the U.S. government, the U.S. Department of the Navy, or the U.S. Naval War College.

I. INTRODUCTION

Peacekeeping is one of the tools used by the United Nations (UN) to maintain or restore international peace and security. Over the years, UN peacekeeping mandates have expanded and diversified in response to the changing character of conflict and the changing needs and expectations of local and international actors. As a result, peacekeeping has become a multidimensional enterprise. Whereas in the early days peacekeeping operations (PKO) were deployed after the end of hostilities, nowadays they are also deployed during active hostilities (international and/or non-international) and are empowered to use lethal force. Most critically, though, they are often deployed in hybrid environments where the dividing line between armed conflict and peace is thin, requiring different responses and standards when using lethal force.

To the extent that the usage of cyber technologies currently shapes the conflict environment within which peacekeeping operates, there is a need to reconsider the means and methods used by peacekeepers to carry out their tasks and, more specifically, consider the "cyberization" of peacekeeping.

For the purposes of this article, we define cyber peacekeeping as the incorporation and use of cyber means and methods by peacekeepers either in the context of a physical peacekeeping operation or in the context of a purely online operation. We also define the use of lethal force in cyber peacekeeping as the use of cyber means to cause death.

The cyberization of peacekeeping inevitably has implications for the legal framework governing peacekeeping and, in particular, the legal framework that regulates the use of lethal force by peacekeepers. These are issues that have received little scholarly attention.[1]

Our purpose in this article is to examine the impact of cyber peacekeeping on the legal framework governing the use of lethal force. More specifically, the article will consider how cyber peacekeeping modulates the use of

1. *See* Nicholas Tsagourias & Giacomo Biggio, *Cyber-Peacekeeping and International Law in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 345–65 (Nicholas Tsagourias & Russell Buchan eds., 2d ed. 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3870713). *See also* Jann Kleffner & Heather Harrison Dinniss, *Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations*, 89 INTERNATIONAL LAW STUDIES 512 (2013).

lethal force under the law of armed conflict and the law enforcement paradigm. The article will focus on cyber peacekeeping operations (CPKO) under UN command and control, but its legal findings will also apply to CPKO deployed by other international organizations as well as traditional peacekeeping operations.

The article is structured in four parts. Part II explains the concept of cyber peacekeeping by providing examples of peacekeeping activities that are or can be "cyberized." The legal basis and principles of peacekeeping will also be discussed in this Part because they provide the backdrop against which the subsequent discussion will unfold. Part III considers the use of lethal force by cyber peacekeepers under the law of armed conflict paradigm based on international humanitarian law (IHL). In this respect, it discusses the applicability of IHL to CPKO and the status of cyber peacekeepers as combatants, civilians, or civilians directly participating in hostilities (DPH). Part IV considers the use of lethal force under the law enforcement paradigm based on international human rights law (IHRL). In this respect, it will consider the extraterritorial applicability of IHRL to CPKO before considering the conditions under which lethal force can be used lawfully according to IHRL. Part V provides a conclusion.

II. THE CONCEPT OF CYBER PEACEKEEPING AND ITS LEGAL BASIS

A. The Concept of Cyber Peacekeeping

According to the UN, peacekeeping is one of the most effective tools it deploys in assisting States to navigate from conflict to peace. It has been defined as "a technique designed to preserve peace, however fragile, where fighting has been halted and to assist in implementing agreements achieved by the peacemakers."[2] As of September 2021, there are twelve active UN missions deploying more than eighty-seven thousand personnel and there have been more than seventy missions since 1948.[3]

---

2. United Nations Peacekeeping Operations Principles and Guidelines 18 (2008), https://www.un.org/ruleoflaw/blog/document/united-nations-peacekeeping-operations-principles-and-guidelines-the-capstone-doctrine/. On peacekeeping, see Rosalyn Higgins et al., *Peacekeeping and other Peace Operations in* OPPENHEIM'S INTERNATIONAL LAW: UNITED NATIONS 1025–92 (Rosalyn Higgins et al. eds., 2017); Michael Bothe, *Peacekeeping in* THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 1171–99 (Bruno Simma et al. eds., 3d ed. 2012).

3. *See* United Nations, Peacekeeping Data, https://peacekeeping.un.org/en/data (as of Sept. 30, 2021).

Over the years, peacekeeping mandates have expanded and diversified to include disarmament and demobilization, conflict prevention, protection of civilians, human rights protection, monitoring violations of humanitarian law, electoral assistance, supporting the re-establishment of rule of law and security institutions, monitoring the implementation of peace agreements, State reconstruction, and reconciliation. Peacekeepers have also been deployed during international and non-international armed conflicts and, indeed, in complex security environments characterized by asymmetric threats. They have also been authorized to use force to carry out their mandate.[4]

Cyber technologies, as we said, not only change the nature of conflict but also the nature of peacekeeping. On the one hand, the use of cyber technologies by parties to a conflict where a PKO is underway can impede the implementation of its mandate. For example, cyber technologies can be used to interfere in elections supervised by peacekeepers; attack infrastructure essential to the civilian population, such as electrical grids or water purification systems; or attack civilians, other parties to the conflict, or the peacekeepers themselves.

On the other hand, cyber technologies can assist peacekeepers to address these challenges and they can be used to facilitate the implementation of their tasks. For example, cyber technologies can assist with the observation, monitoring, and reporting of human rights and international humanitarian law violations; the supervision and monitoring of cease fire agreements or cyber cease-fire agreements; the disarmament and indeed "cyber-disarmament" of parties by ascertaining whether they are destroying conventional weapons or developing new weapons including cyber weapons such as malicious software; and support the electoral process and the building of democratic institutions by monitoring electronic voting or countering the spread of disinformation during elections. Cyber technologies can also be used to thwart cyber-attacks on critical infrastructure systems, civilians, or other parties to the conflict and neutralize "spoilers."[5]

---

4. For example, in relation to the United Nations Multidimensional Integrated Stabilization Mission in Mali, see S.C. Res. 2100 (2013); S.C. Res. 2423 (2018); S.C. Res. 2480 (2019); S.C. Res. 2531 (2020). *See also* UN Peacekeeping Operations Principles and Guidelines, *supra* note 2, at 22.

5. *See* Tsagourias & Biggio, *Cyber-Peacekeeping*, 348–56 *supra* note 1. From a non-legal perspective see Michael Robinson et al., *An Introduction to Cyber Peacekeeping*, 114 JOURNAL OF NETWORK AND COMPUTER APPLICATIONS 70 (2018); A. WALTER DORN, KEEPING WATCH: MONITORING, TECHNOLOGY AND INNOVATION IN UN PEACE OPERATIONS (2011).

The "cyberization" of peacekeeping can also enhance the ability of peacekeepers to perform their tasks. It can assist in improving the decision-making process and the quality of decisions, allow peacekeepers to take quick action, extend the reach of operations, minimize fatalities, and reduce the amount of human, material, and financial resources needed to carry out tasks.

The UN has recognized the importance of cyber technologies for its peacekeeping operations. For instance, the 2015 UN Report of the High-Level Panel on Peace Operations stressed the need for implementing new technologies, including cyber, in peacekeeping operations as a way to promote international security and stability.[6] The UN also established the Office of Information and Communications Technology.[7] One of its initiatives is the Partnership for Technology in Peacekeeping, whose objective is to empower peacekeeping operations through the use of cyber technologies.[8] Certain current missions have already integrated cyber capabilities from intelligence collection to the use of drones.[9]

Although the introduction of cyber technologies in PKO is gaining momentum, it poses a number of institutional, political, and legal challenges. Some of these challenges are discussed by the authors elsewhere[10] but an important challenge relates to the regulation of the use of lethal force in the course of cyber peacekeeping, which is the focus of this article. In the following part, we will consider this issue from the perspective of the law of

---

6. United Nations, Uniting Our Strengths for Peace—Politics, Partnership and People: Report of the High-Level Independent Panel on United Nations Peace Operations paras. 285–87 (June 16, 2015), https://peaceoperationsreview.org/wp-content/uploads/2015/08/HIPPO_Report_1_June_2015.pdf [hereinafter HIPPO Report].

7. *See generally* United Nations Department of Operational Support, Technology, https://operationalsupport.un.org/en/technology (last visited Jan. 28, 2022).

8. *See* United Nations Department of Operational Support, Partnership for Technology in Peacekeeping, https://operationalsupport.un.org/en/partnership-technology-peacekeeping (last visited Jan. 28, 2022).

9. *See, e.g.,* S.C. Res. 2531, ¶ 47 (June 29, 2020) (renewing the Multidimensional Integrated Stabilization Mission in Mali (MINUSMA)):

> [T]ake all appropriate measures to review and enhance the safety and security of MINUSMA's personnel . . . through . . . improving logistics in mission, in particular by taking all necessary measures to secure MINUSMA's logistical supply routes, including through the continued deployment of combat convoy battalions and the use of modern technology such as multiple sensors, intelligence fusion and unmanned aerial systems, as well as by exploring potential alternative logistical supply routes.

10. *See* Tsagourias & Biggio, *Cyber-Peacekeeping*, *supra* note 1, at 363–65.

armed conflict and the law enforcement paradigm, but in order to do this we should first explain the legal framework within which cyber peacekeeping operates because it shapes the legal framework according to which lethal force can be applied in the course of a CPKO.

B. Cyber Peacekeeping: Its Legal Basis and Fundamental Principles

The legal basis of cyber peacekeeping, very much like traditional peacekeeping, is not explicitly stated in the UN Charter. Rather, it can be traced back to the doctrine of implied powers, which has been explained by the International Court of Justice in its *Reparation for Injuries* Advisory Opinion, where the Court held that the United Nations "must be deemed to have those powers which, though not provided expressly in the Charter, are conferred upon it by necessary implications as being essential to the performance of its duties."[11] The Court addressed the lawfulness of peacekeeping operations established by the UN General Assembly in the *Certain Expenses* Advisory Opinion, holding that Article 11 of the UN Charter "empowers the General Assembly, by means of recommendations to States or to the Security Council, or to both, to organize peacekeeping operations, at the request, or with the consent, of the States concerned."[12] The Court also opined that peacekeeping is a means for attaining the UN purposes of maintaining international peace and security and that it is not equivalent to peace enforcement.[13]

It follows from this advisory opinion that a CPKO can be established by the General Assembly on the basis of Articles 10, 11, 12, and 22 of the UN Charter, which endow it with general and broad recommendatory powers on matters relating to international peace and security. A CPKO can also be established by the Security Council in order to fulfil its "primary responsibility for the maintenance of international peace and security."[14] More specifically, the Security Council can recommend the establishment of a CPKO in the exercise of its Chapter VI powers[15] or mandate its establishment in the exercise of its Chapter VII powers.[16] Although the theory of implied powers

11. Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion, 1949 I.C.J. 174, 182 (Apr. 11).

12. Certain Expenses of the United Nations, Advisory Opinion, 1962 I.C.J. 151, 164 (July 20).

13. *Id.* at 163–68.

14. U.N. Charter art. 24.

15. U.N. Charter art. 36.

16. U.N. Charter arts. 39–42.

provides a sound legal basis for establishing a CPKO by the Security Council, Article 41 of the UN Charter, in our opinion, provides a more concrete legal basis. That article allows the Security Council to take a variety of measures not involving the use of force in the sense of Article 42 of the Charter.[17] A CPKO can be such a measure because, as we will explain later, it is not an Article 42 peace enforcement operation, even if it is authorized to use force.

This leads us to discuss the principles that define peacekeeping and CPKO and which have a bearing on the use of lethal force. We refer here to the principles of host State consent, impartiality, and use of force in self-defence.[18] Host State consent provides the legal basis for the establishment and deployment of a CPKO recommend by the General Assembly or the Security Council. Regarding CPKOs established by the Security Council based on a Chapter VII binding resolution,[19] host State consent is not a prerequisite for its establishment but necessary for its deployment. This is because, otherwise, its deployment will violate Article 2(7) of the UN Charter, which prohibits UN interference in the domestic affairs of States.[20] This provision exempts Article 42 enforcement operations but as will be explained shortly, peacekeeping is not enforcement. In the absence of host State consent, cyber peacekeeping activities, such as surveillance of the State's networks or systems, be it for the purposes of implementing a cyber cease-fire agreement or for conducting cyber disarmament operations or for protecting

17. U.N. Charter art. 41. *See also* Prosecutor v. Tadić, Case No. IT-94-1-AR-72, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 35 (Int'l Crim. Trib. for the former Yugoslavia Oct. 2, 1995); Certain Expenses of the United Nations, Advisory Opinion, 1962 I.C.J. 151, 166, 171 (July 20).

18. UN Peacekeeping Operations Principles and Guidelines, *supra* note 2, at 31–36; United Nations, Report of the Panel on United Nations Peace Operations, ¶¶ 45–55, U.N. Doc. A/55/305–S/2000/809 (Aug. 2, 2000), https://www.un.org/ruleoflaw/files/brahimi%20report%20peacekeeping.pdf [hereinafter Brahimi Report]; HIPPO Report, *supra* note 6, paras. 124–30; United Nations, Principles of Peacekeeping, https://peacekeeping.un.org/en/principles-of-peacekeeping (last visited Jan. 28, 2022). Prosecutor v. Sesay, Kallon, and Gbao, Case No. SCSL-04-15-T, Trial Judgment, ¶ 225 (Special Court for Sierra Leone Mar. 2, 2009); Prosecutor v. Abu Garda, Case No. ICC-02/05-02/09, Decision on the Confirmation of Charges, ¶ 71 (Feb. 8, 2010). *See also* Nicholas Tsagourias, *Consent, Neutrality/Impartiality and Self-Defence in Peacekeeping: Their Constitutional Dimension*, 11 JOURNAL OF CONFLICT AND SECURITY LAW 465 (2006).

19. U.N. Charter art. 25, 103; Tsagourias, *Consent, Neutrality/Impartiality and Self-Defence in Peacekeeping*, *supra* note 18, at 471, 477. For a detailed exposition, see also Patryk I. Labuda, *UN Peacekeeping as Intervention by Invitation: Host State Consent and the Use of Force in United Nations-Mandated Stabilisation Missions*, 7 JOURNAL ON THE USE OF FORCE AND INTERNATIONAL LAW 317 (2020).

20. U.N. Charter art. 2(7).

critical national infrastructures from cyber-attacks, will violate that State's domestic jurisdiction.

The principle of impartiality, the second principle, is an operational term meaning that a CPKO should execute its tasks "without favour or prejudice" to any party in accordance with the mission's mandate.[21]

Finally, cyber peacekeepers can use force in personal self-defence, in defence of others (such as civilians), or in order to defend the CPKO's mandate, which often leads to the proactive use of force.[22] The defensive use of force is critical in distinguishing a peacekeeping operation from an Article 42 peace-enforcement operation. In peacekeeping, the use of force is incidental and limited to achieving the mandate's specific objectives, whereas in peace enforcement the use of force is central to the operation and is used to achieve broader strategic objectives. The fact that the Security Council is nowadays authorizing peacekeepers to use force does not transform the operation into peace enforcement. Security Council authorization is required because such use of force goes beyond what is required for personal defence or the defence of others.[23] It should be recalled in this regard that the Security Council often mentions self-defence explicitly when granting such authorization.[24] The difference between a PKO authorized to use force and a peace-enforcement operation is also demonstrated by the fact that a PKO is deployed on

---

21. UN Peacekeeping Operations Principles and Guidelines, *supra* note 2, at 33; Brahimi Report, *supra* note 18, paras. 48–50; Prosecutor v. Sesay, Kallon, and Gabo, Case No. SCSL-04-15-T, Trial Judgment, ¶ 277 (Special Court for Sierra Leone Mar. 2, 2009); Prosecutor v. Abu Garda, Case no. ICC-02/05-02/09, Decision on the Confirmation of Charges, ¶ 73 (Feb. 8, 2010). On the principle of impartiality, see generally Hikaru Yamashita, "*Impartial" Use of Force in United Nations Peacekeeping*, 15 INTERNATIONAL PEACEKEEPING 615 (2008).

22. *See* Brahimi Report, *supra* note 18, para. 55; HIPPO Report, *supra* note 6, paras. 124, 128. Carlos Alberto dos Santos Cruz et al., Improving Security of United Nations Peacekeepers: We Need to Change the Way We are Doing Business (Dec. 19, 2017), https://peacekeeping.un.org/sites/default/files/improving_security_of_united_nations_peacekeepers_report.pdf; The Kigali Principles on the Protection of Civilians princ. 3 (2015). *See also* Scott Sheeran, *Use of Force in United Nations Peacekeeping Operations*, *in* THE OXFORD HANDBOOK ON THE USE OF FORCE IN INTERNATIONAL LAW 347 (Marc Weller ed., 2011); Nicholas Tsagourias, *Self-Defence, Protection of Humanitarian Values, and the Doctrine of Neutrality and Impartiality in Enforcement Mandates*, *in id.* at 398–415.

23. Authorization is also needed because States or international organizations may have different approaches or laws regarding to the use of force in self-defence.

24. It should be noted, however, that the line between peacekeeping and peace enforcement has sometimes been crossed as with the Force Intervention Brigade in the context of the UN Stabilization Mission in the Democratic Republic of the Congo. *See* S.C. Res. 2098, ¶ 12(b) (Mar. 28, 2013); S.C. Res. 2147, ¶ 4(b) (Mar. 28, 2014); S.C. Res. 2211, ¶ 9(e) (Mar. 26, 2015).

the basis of State consent whereas peace enforcement operations are launched against the will of the targeted State.

If cyber peacekeepers are empowered to use force in self-defence, the defence of others, or the defence of the mandate, the next issue to discuss is whether the applicable legal framework for their use of lethal force is the law of armed conflict or the law enforcement paradigm.

III. THE USE OF LETHAL FORCE BY CYBER PEACEKEEPERS UNDER THE LAW OF ARMED CONFLICT PARADIGM

The use of lethal force under the law of armed conflict paradigm is regulated by IHL which as *lex specialis* is dispositive of the situation.[25] More specifically it is governed by the principle of distinction according to which combatants can be lawfully targeted at all times whereas civilians are protected from attacks unless they directly participate in hostilities.[26]

The application of the armed conflict paradigm depends on whether there is an international (IAC) or a non-international (NIAC) armed conflict to which the CPKO has become a party. An armed conflict exists when there is "resort to armed force," that is, resort to acts of violence which cause or are intended to cause damage or destruction to objects or death and injury to individuals.[27] Furthermore, an IAC exists when there is resort to armed

25. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J 226, ¶ 25 (July 8); Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 106 (July 9).

26. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts arts. 48–58, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I]; Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts art. 13, June 8, 1977, 1125 U.N.T.S. 609. 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW r. 1–10 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005); Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J 226, ¶¶ 78–79 (July 8). *See also* INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW (2009) [hereinafter DPH GUIDANCE].

27. Prosecutor v. Tadić, Case No. IT-94-1-AR-72, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the former Yugoslavia Oct. 2, 1995); OFFICE OF THE GENERAL COUNSEL, U.S. DEPARTMENT OF DEFENSE, LAW OF WAR MANUAL § 3.3.1 (rev. ed. Dec. 2016) [hereinafter DOD LAW OF WAR MANUAL].

force between States[28] whereas a NIAC exists when there is "protracted armed violence between governmental authorities and organized armed groups or between such groups."[29] The above classifications also apply to the involvement in armed conflicts of international organizations such as the UN.[30]

The next issue to consider is when a UN CPKO becomes a party to an IAC or NIAC, but before we do, it is important to make three preliminary observations. The first recognizes that the UN has been reluctant to formally acknowledge that its peacekeeping forces can become a party to an armed conflict and subject to IHL, preferring to treat them as civilians. This view does not, however, comport with the facts on the ground where UN peacekeepers are involved in hostilities.[31] Neither does it comport with the principle of distinction mentioned above or the principle of equality of belligerents, according to which IHL should apply equally to all parties to an armed conflict. Although the UN is gradually changing its approach, the issue of whether IHL applies to UN peacekeeping forces is fraught with difficulties due to the absence of a formal UN position.[32] The second observation refers to the fact that the existence of an armed conflict and whether a PKO becomes a party to the armed conflict are factual questions and do not depend on the character or the mandate of the operation or its legal basis.[33] The third

28. Common Article 2 to the Geneva Conventions of 1949. *See also* Tristan Ferraro & Lindsey Cameron, *Article 2: Application of the Convention*, *in* 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 THE ARMED FORCES IN THE FIELD, ¶¶ 201–317 (2016); *Tadić*, ¶ 70.

29. *Tadić*, ¶ 70. *See also* Common Article 3 to the Geneva Conventions of 1949; Lindsey Cameron et al., *Article 3: Conflicts Not of an International Character*, *in* 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, ¶¶ 384–504 (2016); Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts art. 1(1), June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II].

30. *See also* Tristan Ferraro, *The Applicability of International Humanitarian Law to Multinational Forces*, 95 INTERNATIONAL REVIEW OF THE RED CROSS 561, 575, 578–79 (2013).

31. In relation to the UN Multidimensional Integrated Stabilization Mission in Mali, see the Secretary-General's Report on the Situation in Mali, ¶¶ 95–97, U.N. Doc. S/2020/1281 (Dec. 28, 2020).

32. HIPPO Report, *supra* note 6, para. 122.

33. *Article 2* and *Article 3* (respectively), *in* 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, ¶¶ 211, 411 (2016).

and final observation is that peacekeeping operations, including CPKO, consist of military personnel (military units/contingents) as well as civilian personnel (for example, police units). These units operate under different command structures but sometimes under integrated command. Recognizing the dual composition (military and civilian) of a CPKO is important for determining which component becomes a party to an armed conflict and under what circumstances lethal force can be lawfully used.

A. Cyber Peacekeepers as Party to an IAC and Their Status

A CPKO which is deployed during an IAC will become a party to that armed conflict from the moment it resorts to acts of cyber violence against opposing parties. These include acts that cause death, injury, destruction, or damage. This will be the case, for example, when it targets opposing parties' soldiers or destroys their networks through cyber means.[34] In the absence of a pre-existing IAC, a CPKO can trigger an IAC if it launches cyber operations which produce effects similar to those described above.[35] It should be noted in this respect that it is the collective, organized, and war-like nature of cyber operations that will render the CPKO a party to an IAC because they are removed from the ambit of personal self-defence or defence of others. In contrast, random and unauthorized violent acts by individual peacekeepers may amount to direct participation in hostilities if they cross the threshold of self-defence but they will not make the CPKO a party to an armed conflict.[36]

Whether the exchange of violence between cyber peacekeepers and other parties should reach a certain level of intensity has been the subject of debate. There are legal and policy reasons supporting a minimum threshold, including the need to establish some parity with NIACs, but the overwhelming view is that any occurrence of violence, regardless of intensity, can trigger an IAC.[37] In the cyber peacekeeping context, this raises the question of

34. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS r. 82, 83, at 379–91 (Michael N. Schmitt gen. ed., 2017) [hereinafter TALLINN MANUAL 2.0].

35. *Id.*

36. What constitutes DPH and how it applies to cyber peacekeepers will be discussed in Section III.C.

37. International Law Association, *Final Report on the Meaning of Armed Conflict in International Law* 2, 30, 32 (2010), http://www.rulac.org/assets/downloads/ILA_report_armed_conflict_2010.pdf.

whether cyber-operations that cause disruptive effects—for instance, by impairing the functionality of the targeted computer network or systems—can trigger an IAC. The prevailing view is that they would not.[38]

If a UN CPKO becomes a party to an IAC, customary IHL, including the principle of distinction, will govern the use of lethal force.[39] This is because the UN, as an international legal person, is bound by customary IHL.[40] It is therefore important to determine the status of cyber peacekeepers under IHL and, more specifically, whether they become combatants or remain civilians in view of the fact that a cyber peacekeeping force may consist of military as well as civilian units.

The UN has dealt with this issue in a 1999 Bulletin by the UN Secretary-General. According to the Bulletin:

> The fundamental principles and rules of international humanitarian law . . . are applicable to United Nations forces when in situations of armed conflict they are actively engaged therein as combatants, to the extent and for the duration of their engagement. They are accordingly applicable in enforcement actions, or in peacekeeping operations when the use of force is permitted in self-defence.[41]

The Bulletin seems to introduce a notion of "quasi combatancy," according to which peacekeepers (including military personnel) can be lawfully targeted only as long as they actively engage in hostilities; otherwise they are

38. TALLINN MANUAL 2.0, *supra* note 34, at 376–77, 384. *See also* Federal Government of Germany, On the Application of International Law in Cyberspace, Position Paper, at 7 (Mar. 2021) [hereinafter German Position Paper], https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf; French Ministry of the Armies, International Law Applied to Operations in Cyberspace 12 (Sept. 9, 2019).

39. *The Applicability of International Humanitarian Law in Peace Operations*, *in* LEUVEN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO PEACE OPERATIONS 91 (Terry Gill et al. eds., 2017).

40. Interpretation of the Agreement of 25 March 1951 between the WHO and Egypt, Advisory Opinion, 1980 I.C.J. 78, 89–90 (Dec. 20); Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion, 1949 I.C.J. 174, 179 (Apr. 11). *Contra* DOD LAW OF WAR MANUAL, *supra* note 27, § 18.1.4.

41. U.N. Secretary-General's Bulletin, Observance by United Nations Forces of International Humanitarian Law, U.N. Doc. ST/SGB/1999/13, at 1.1 (Aug. 6, 1999). *See also* Convention on the Safety of United Nations and Associated Personnel art. 2(2), Dec. 15, 1994, 2051 U.N.T.S. 363.

entitled to the protection accorded to civilians.[42] It also applies this principle to individual peacekeepers and not collectively to the contingent. In our opinion, the Bulletin's approach is unwarranted for many reasons. First, it undermines the principle of distinction and the collective classification of those caught in an armed conflict, but also limits the application of IHL to situations of active engagement in hostilities excluding defensive acts of violence.[43] Second, it overlooks factual situations characterized by intense fighting between peacekeepers and other parties and, instead, relies on the mandate and the purpose of the operation. Third, it limits the application of IHL to situations where there is already an armed conflict. Fourth, it undermines the principle of equality of belligerents by treating peacekeepers as quasi or part-time combatants. Fifth, it creates uncertainty as to what law—IHRL or IHL—will apply to any given use of lethal force as well as what law will apply at any time to the civilian or military personnel of a CPKO by introducing a revolving door scenario, even for military personnel.

We thus submit that when a CPKO becomes a party to an IAC, its military personnel collectively become combatants until they are withdrawn or until the conflict ends.[44] Consequently, they can be lawfully targeted at any time, but they can also lawfully target other combatants. The civilian personnel of a CPKO will instead remain immune from attacks unless and for as long as they commit DPH, as will be explained in Section III.C. [45]

B. Cyber Peacekeepers as Party to a NIAC

A CPKO will become a party to a NIAC if there is resort to armed force with armed groups and the two defining criteria of a NIAC—organization

---

42. *See also* Prosecutor v. Sesay, Kallon, and Gbao, Case No. SCSL-04-15-T, Trial Judgment, ¶ 233 (Special Court for Sierra Leone Mar. 2, 2009); Prosecutor v. Abu Garda, Case No. ICC-02/05-02/09, Decision on the Confirmation of Charges, ¶ 83 (Feb. 8, 2010).

43. See, for example, how the principle of distinction regulates attacks which are defined according to Additional Protocol I, Article 49(1) as "acts of violence against the adversary, whether in offence or in defence."

44. INTERNATIONAL HUMANITARIAN LAW: CASES, MATERIALS AND COMMENTARY 108, para. 8 (Nicholas Tsagourias & Alasdair Morrison eds., 2018). HIPPO Report, *supra* note 6, para. 122; Ferraro, *supra* note 30, at 600–5; Dieter Fleck, *The Legal Status of Personnel Involved in the United Nations Peace Operations,* 95 INTERNATIONAL REVIEW OF THE RED CROSS 613 (2013). DANISH MINISTRY OF DEFENCE, MILITARY MANUAL ON INTERNATIONAL LAW RELEVANT TO DANISH ARMED FORCES IN INTERNATIONAL OPERATIONS para. 5.5 (2016).

45. 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW r. 33 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005).

of the parties and intensity of the conflict—are fulfilled.[46] These customary law criteria, drawn from Common Article 3 of the Geneva Conventions and international jurisprudence,[47] differ in certain respects from the criteria laid down in Additional Protocol II to the Geneva Conventions but they will apply to CPKO to the extent that the Additional Protocol II criteria have not reached customary law status.

International jurisprudence has indicated a number of factors to be taken into consideration when assessing the existence of these two criteria.[48] In relation to organization, relevant factors include the existence of a command structure; the group's ability to carry out operations in an organized manner; the level of logistics; the degree of discipline; the ability to implement IHL; and factors relating to the group's ability to speak with one voice.[49] The military contingent of a CPKO will satisfy this criterion because organization is the defining feature of any military force. Even an online CPKO established by the UN and composed of military personnel will satisfy this criterion because it will be integrated within the UN's line of political and military command.

Turning now to the criterion of intensity, relevant factors that can be considered are the number, duration, and intensity of confrontations; the seriousness of the attacks; the type of weapons used; the spread of the attacks over territory and time; the type of forces partaking in the fighting; the number of casualties; the extent of material destruction; and the involvement of the UN Security Council.[50]

---

46. Whether organization and intensity should be treated as the defining criteria or whether the broader circumstances of the armed conflict should be taken into consideration is debated. However, for the purposes of this article, we will still use these two criteria as the determining factors of a NIAC. *See, e.g.*, Jann K. Kleffner, *The Legal Fog of an Illusion: Three Reflections on "Organization" and "Intensity" as Criteria for the Temporal Scope of the Law of Non-International Armed Conflict*, 95 INTERNATIONAL LEGAL STUDIES 161, 168–77 (2019).

47. *See, e.g.*, Prosecutor v. Limaj, Case No. IT-03-66-T, Judgment, ¶¶ 93–174 (Int'l Crim. Trib. for the former Yugoslavia Nov. 30, 2005); Prosecutor v. Haradinaj, Case No. IT-04-84-T, Judgment, ¶¶ 37–62 (Int'l Crim. Trib. for the former Yugoslavia Apr. 3, 2008); Prosecutor v. Boškoski and Tarčulovski, Case No. IT-04-82-T, Judgment, ¶¶ 175–77, 195–203 (Int'l Crim. Trib. for the former Yugoslavia July 10, 2008); Prosecutor v. Bemba Gombo, Case No. ICC-01/05-01/08, Judgment, ¶¶ 137–40 (Mar. 21, 2016); Prosecutor v. Thomas Lubanga Dyilo, Case No. ICC-01/04-01/06-2842, Judgment, ¶ 537 (Mar. 14, 2012).

48. *Prosecutor v. Boškoski and Tarčulovski*, ¶¶ 177, 197.

49. *Id.* ¶¶ 199–203. *Prosecutor v. Limaj*, ¶ 64; *Prosecutor v. Thomas Lubanga Dyilo*, ¶ 537.

50. *Prosecutor v. Bemba Gombo*, ¶ 137; *Prosecutor v. Limaj*, ¶ 394; *Prosecutor v. Haradinaj*, ¶ 49; *Prosecutor v. Boškoski*, ¶ 177. *See also* DOD LAW OF WAR MANUAL, *supra* note 27, § 3.4.2.2.

Whether cyber-attacks launched by cyber peacekeepers can reach the required level of intensity to trigger a NIAC is theoretically possible but factually rather unlikely.[51]As France opined, "the state of technology seems for the time being to rule out the possibility that cyberoperations alone reaching the necessary threshold of violence to characterise a NIAC situation."[52] A similar view was taken by Germany, which considers that "activities such as large-scale intrusion into foreign cyber systems, significant data theft, the blocking of internet services and the defacing of governmental channels or websites will usually not singularly and in themselves bring about a non-international armed conflict."[53]

It follows from the above that the situations under which a CPKO will become a party to a NIAC are limited. Therefore, a CPKO's use of lethal force will typically be regulated by the law enforcement paradigm, as will be explained in Part IV. That notwithstanding, one can envisage situations where a CPKO can become a party to a NIAC when, for example, kinetic and cyber force are used in tandem leading to cumulative intensity or when a CPKO is part of a physical peacekeeping operation which has become a party to an NIAC through the use of kinetic force.

In addition to the above, the support-based approach (SBA) introduced by the International Committee of the Red Cross (ICRC) becomes relevant in cases where the CPKO's own participation is not sufficient to make it a party to a NIAC.[54]

According to the support-based approach, a multinational force, in our case a cyber peacekeeping force, will become a party to a NIAC if four conditions are met. First, there must be a pre-existing NIAC taking place on the territory where the third power (CPKO) intervenes. Second, actions related to the conduct of hostilities are undertaken by the intervening power (CPKO) in the context of that pre-existing conflict. Third, the military operations of the intervening power (CPKO) are carried out in support of one of the parties to the pre-existing NIAC. Finally, the action in question is

51. See in this regard TALLINN MANUAL 2.0, *supra* note 34, at 383–84.

52. French Ministry of the Armies, *supra* note 38, at 12.

53. German Position Paper, *supra* note 38, at 7.

54. *See* Tristan Ferraro, *The ICRC's Legal Position on the Notion of Armed Conflict Involving Foreign Intervention and on Determining the IHL Applicable to this Type of Conflict*, 97 INTERNATIONAL REVIEW OF THE RED CROSS 1227 (2015). *See also* Ferraro, *supra* note 30, at 561–612.

undertaken pursuant to an official decision by the intervening power (UN) to support a party involved in the pre-existing conflict.[55]

It is important therefore to consider what type of support can render a CPKO a party to a pre-existing NIAC under a support-based approach. It should be noted that the ICRC does not provide any further explanation, but the "decisive element" would be the contribution made by the CPKO to the conduct of hostilities, and more specifically, whether its actions have "a direct impact on the opposing party's ability to carry out military operations."[56]

For instance, if a CPKO uses lethal force against armed groups fighting the government, this will render it a party to the NIAC. The execution of other tasks may not, however, necessarily yield the same outcome. Suppose that the CPKO, while performing observance, monitoring, and reporting duties, provides the government with intelligence information about imminent attacks on civilians or governmental forces. Will the CPKO become a party to a NIAC under this scenario? For the ICRC, "intelligence activities" may indeed constitute involvement in hostilities, so it depends on whether they are directed at the enemy or are at least "closely related to action against the enemy."[57] If the provided information was specific, identifying, for example, the location of a threat actor who is then targeted, it will make the CPKO a party to the NIAC, but would that be the case if the supported party (government) does not act upon this information? If the information is general, one can reasonably say that it will not satisfy this criterion. However, even in this case the opposing party may be affected if the supported party (government) would not otherwise have had access to any information. Also, would a clear distinction be made between the provision of tactical intelligence to support defensive or offensive operations and strategic intelligence? One could say that, cumulatively, the provision of information or intelligence may have a direct impact on the other party.

This leads us to another set of questions: should the impact of the action be ascertained objectively on the basis of facts or in the abstract (presumed and potential impact)? Should the actual use of the provided support be taken into consideration? Should the intention of the CPKO in providing

55. International Committee of the Red Cross, Report on International Humanitarian Law and the Challenges of Contemporary Conflicts 1231, (Oct. 31, 2015), https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts.

56. Ferraro, *supra* note 30, at 585.

57. *Id.* at 586 n.73.

support be taken into consideration? For example, if information is provided to the government which is used against the wishes of the CPKO, would that make the CPKO a party to a NIAC? Also, if information is provided in violation of the CPKO mandate, would that make it a party to a NIAC?

According to the third support-based approach criterion, the military operations must be carried out in support of one of the parties to the pre-existing conflict. Since the principle of impartiality, according to which a CPKO should treat all parties equally and should not support one party to the detriment of the other, informs peacekeeping, this criterion cannot in principle be fulfilled. This finding is not affected by the other peacekeeping principle, namely, the consent of the government, because such consent is necessary for the establishment and deployment of the CPKO, as we said, whereas the conduct of the CPKO is regulated by the principle of impartiality notwithstanding the government's consent. The only instance where impartiality may be dispensed with, and the third support-based approach criterion be fulfilled, is when the mandate requires the CPKO to cooperate with the government or support the government to achieve certain objectives and the CPKO actually does so. This also relates to the question mentioned above of whether the detrimental effect of support should be factually established or be presumed.

A separate question regarding the support-based approach is whether support provided to armed groups participating in a NIAC or to other international organizations or participating States would make a CPKO party to the NIAC. For example, the UN Multidimensional Integrated Stabilization Mission in the Central African Republic was requested to provide support to the Joint Force of the Group of Five for the Sahel involving, among other things, intelligence sharing[58] and was requested to exchange intelligence with the French forces in Mali.[59] This is an important question because the ICRC limits the support-based approach to support provided to the government of the State. As we also said, peacekeeping is informed by the principle of impartiality. If, for example, one of the CPKO's tasks is to protect civilians from attacks, it should equally protect them from attacks launched by governmental forces, armed groups, or other forces. For this reason, it may need to share information with any of the above parties. Such support may even be mandated by the Security Council, as we have seen. It appears then that

58. S.C. Res. 2359, ¶ 5 (June 21, 2017).
59. S.C. Res. 2423, ¶ 41 (June 28, 2018).

the support-based approach creates legal gaps. In our opinion, nothing precludes the application of a support-based approach to support provided to other actors such as armed groups. Consequently, a CPKO may become a party to a NIAC involving a government (supported by other States or international organizations) and an armed group, or a NIAC involving armed groups, or become party to both if more than one NIAC exists.

The preceding discussion has revealed the challenges and gaps surrounding the support-based approach as formulated by the ICRC. The support-based approach can also be criticized on many other grounds. First, it renders an entity a party to an armed conflict on the basis of assistance, similar to the criminal law concept of joint criminal enterprise. This is contrary to the established approach, according to which the existence of an armed conflict, its categorization, and whether an entity becomes party thereto depend on the bilateral relations between entities involving exchanges of violence. Second, by lowering the threshold for applying the law of NIAC to peacekeepers or other multilateral forces, it creates legal inequality between the parties involved in an armed conflict. Third, it makes the distinction between acts of violence linked to an armed conflict and those not related to an armed conflict difficult to maintain. Fourth, it is hardly reconcilable with the nature and the mandates of peacekeeping operations and can adversely affect their future deployment in the course of NIACs.[60] Finally, the support-based approach is not based on a firm legal basis nor have States expressed their support.[61]

For these reasons, we reject the support-based approach and revert to the traditional criteria for establishing the existence of a NIAC which should apply to a CPKO.

60. The ICRC's aim to curb foreign interventions in NIACs would have detrimental effects on PKO.

61. For criticism see Marten Zwanenburg, *Double Trouble: The "Cumulative Approach" and the "Support-based Approach" in the Relationship Between Non-State Armed Groups*, 22 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 57 (2019); Terry Gill, *Some Thoughts on the ICRC Support Based Approach*, QUESTIONS OF INTERNATIONAL LAW (May 13, 2019), http://www.qil-qdi.org/some-thoughts-on-the-icrc-support-based-approach/; LEUVEN MANUAL, *supra* note 39, at 103.

C. The Status of Cyber Peacekeepers in NIACs: Between Combatancy and Direct Participation in Hostilities

The issue to discuss in this section is whether, in cases where a CPKO becomes party to a NIAC, cyber peacekeepers become combatants or remain civilians protected from attacks unless they commit DPH. IHL protects civilians caught in a NIAC[62] and, although the status of combatant does not formally exist in NIACs, international jurisprudence and practice have accepted that the principle of distinction applies.[63] A civilian in a NIAC is defined negatively as "anyone who is not a member of the armed forces or of an organized military group belonging to a party to the conflict"[64] from which the definition of combatant, or its equivalent such as "fighter," can be extrapolated. That said, whereas membership of governmental forces can be easily established, in relation to armed groups the question is whether it is membership or continuous combatant function that renders them targetable.[65] The ICRC opts for the latter[66] but in our opinion the former, membership, is preferrable.[67] It follows from this that the members of the military unit of a CPKO which has become a party to a NIAC become combatants

62. AP II, *supra* note 29, art. 13.

63. 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW r. 5 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005); MICHAEL N. SCHMITT, CHARLES H. B. GARRAWAY & YORAM DINSTEIN, THE MANUAL ON THE LAW OF NON-INTERNATIONAL ARMED CONFLICT WITH COMMENTARY 4–5 (2006), http://www.dur.ac.uk/resources/law/NIACManualIYBHR15th.pdf; Jann Kleffner, *From "Belligerents" to "Fighters" and Civilians Directly Participating in Hostilities—On the Principle of Distinction in Non-International Armed Conflict One Hundred Years after the Second Hague Peace Conference,* 54 NETHERLANDS INTERNATIONAL LAW REVIEW 323 (2007).

64. Prosecutor v. Galić, Case No. IT-98-29-T, Judgment, ¶ 47 (Int'l Crim. Trib. for the former Yugoslavia Dec. 5, 2003); Prosecutor v. Blaškić, Case No. IT-95-14-A, Appeals Chamber Judgment, ¶¶ 110–13 (Int'l Crim. Trib. for the former Yugoslavia July 29, 2004). *See also* AP I, *supra* note 26, arts. 43, 50. As the International Criminal Tribunal for the former Yugoslavia opined "To determine the scope of civilian population in Article 5 of the Statute of the Tribunal, the Appeals Chamber must have been fully aware that this Article contains a statutory armed conflict requirement in which the international or internal character of the conflict is immaterial." Prosecutor v. Mrkšić et al., Case No. IT-95-13/1, Trial Chamber Judgment, ¶ 456 (Int'l Crim. Trib. for the former Yugoslavia Sept. 27, 2007); DPH GUIDANCE, *supra* note 26, at 27.

65. DOD LAW OF WAR MANUAL, *supra* note 27, § 5.7.3.

66. DPH GUIDANCE, *supra* note 26, at 27–37.

67. Tsagourias & Morrison eds., *supra* note 44, at 107, 287–88 (paragraphs 4 and 5, respectively). YORAM DINSTEIN, NON-INTERNATIONAL ARMED CONFLICTS IN INTERNATIONAL LAW (2d ed. 2021), at 77–78, ¶¶ 208–10.

and retain this status for the duration of the NIAC or until they withdraw. This approach adheres to the principle of equality of belligerents and the principle of distinction because it does away with the notion of quasi-combatants, quasi-civilians, or the revolving door scenario.

Regarding the CPKO's civilian personnel, they will be protected from attacks but forfeit their civilian protection for as long as they commit DPH.[68] This is a particularly salient point in the context of cyber peacekeeping because, due to the nature of cyber technologies, civilians, such as technical experts, can support the military.

For this reason, we will consider under what circumstances civilian members of a CPKO lose their civilian protection by committing DPH after making two points. The first point is that DPH applies to IACs as well as NIACs but also to situations where a CPKO has not become a party to an armed conflict. The second point is that DPH relates to random or spontaneous participation of civilians in hostilities in contrast to the collective and organized participation of armed forces.

Moving now to the DPH criteria, according to the ICRC's *Interpretive Guidance on the Notion of Direct Participation in Hostilities*, the following three criteria should be fulfilled: threshold of harm; direct causation; and belligerent nexus.[69]

How do these criteria apply to cyber peacekeepers? Regarding the threshold of harm, according to the ICRC's *Interpretive Guidance* the act must be likely to adversely affect the military operations or capacity of a party to the armed conflict or inflict death, injury, or destruction on protected persons or objects. Suppose that a civilian member of a CPKO detects malicious cyber activity and traces the activity to networks used by a party to the armed conflict, for example an armed group or the government. That civilian then

68. AP II, *supra* note 29, art. 13(3).

69. DPH GUIDANCE, *supra* note 26, at 46–64. *See also* TALLINN MANUAL 2.0, *supra* note 34, r. 97; MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 202–11 (2014). For a general critique of the ICRC *Interpretive Guidance* see Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW & POLICY 641–93 (2010); Michael N. Schmitt, *Deconstructing Direct Participation in Hostilities: The Constitutive Elements,* 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW & POLICY 697 (2010); William H. Boothby, *"And For Such Time As": The Time Dimension to Direct Participation in Hostilities*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW & POLICY 741 (2010); W. Hays Parks, *Part IX of the ICRC "Direct Participation in Hostilities" Study: No Mandate, No Expertise, and Legally Incorrect,* 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW & POLICY 770 (2010).

goes on to disable the network. In this case, the act affects the cyber-capabilities of the targeted party and would satisfy the threshold of harm requirement. Likewise, if the civilian cyber peacekeeper's operation results in physical destruction, for example the destruction of the network or an explosion that injures or kills the opposing party, the threshold of harm requirement is met. Conversely, if the attack disables or disrupts the State's civilian servers in order to affect the operations of an armed group, this requirement will not be met unless the armed group's networks are connected to the State servers. Similarly, intelligence gathering, or sharing, will not satisfy this requirement unless it is linked to a specific harmful attack.

Turning now to the second criterion, that of direct causation, according to the ICRC's *Interpretive Guidance* the harm should be brought about in one causal step. Causal proximity must not be confused with temporal or geographical proximity; for this reason cyber-operations conducted remotely can theoretically satisfy this criterion.[70] However, this test is hard to meet as cyber operations often produce delayed or reverberating effects.[71] In the example given above, if the relevant act consisted of the insertion of a logic bomb to the opponent's networks to be activated at a later time, the causal link between the act and the consequences will not be met.

To use another example, a civilian member of a CPKO launches a cyber operation to disrupt the operating system of an electricity station which provides electricity to a building where members of an armed group operate. This causes a power outage which results in a fire killing several members of the armed group. The cyber-operation in question meets the threshold of harm because it adversely affects the military capacity of a party to the armed conflict and causes death or injury to individuals. However, since its harmful effects are not produced in a single causal step, it will not satisfy the direct causation test. Neither will intelligence sharing, or provision of logistics meet this test unless it is specific and is acted upon. For example, if a civilian cyber peacekeeper supplies governmental forces tactical intelligence on enemy armed groups that then go on to attack them, it will satisfy the criterion of causation but not if it involves strategic intelligence.

---

70. DPH GUIDANCE, *supra* note 26, at 55.

71. Reverberating effects, also referred to as "indirect effects," are "the delayed and displaced second-, third-, and higher-order consequences of action, created through intermediate events or mechanisms." See, in this regard, Chairman, Joint Chiefs of Staff, Joint Publication 3-60, Joint Targeting, ¶ II-35 (2007).

In order to avoid the difficulties the causal test poses to cyber operations, we are of the opinion that it should be interpreted more expansively to include all events in an uninterrupted causal chain, where each event would not have happened "but for" the event that immediately preceded it.[72] Put differently, if the harm can be seamlessly linked to the cyber act, a causal link will be established. Under this approach, the cyber-attacks in the examples mentioned above will satisfy the causation test. However, it should be noted that this approach goes beyond the ICRC's position.

There is another issue that needs to be discussed in relation to the causal test. Cyber-attacks usually consist of compositive acts: preparation, reconnaissance, exploitation, and execution. The question then is whether these acts viewed as a whole can satisfy the causality test. According to the ICRC's *Interpretive Guidance*, composite acts will satisfy this test if they are "an integral part of a concrete and coordinated tactical operation that directly causes such harm."[73] This would mean that a civilian cyber peacekeeper who engages in cyber reconnaissance to identify exploitable vulnerabilities will be committing DPH if reconnaissance was integral to the subsequent cyber-attack. If the act of reconnaissance were to be assessed individually, it would have been difficult to link it to the harmful act. [74]

Finally, according to the third criterion, the belligerent nexus, the act must be specifically designed to cause harm in support of a party to the armed conflict and to the detriment of another.[75] The ICRC *Interpretive Guidance*, however, excludes acts in personal self-defence and the defence of others.[76] This means that harmful acts by cyber peacekeepers in personal self-defence or the defence of others (civilians) will be excluded. It will also cover sporadic acts to defend its military personnel provided that the cyber peacekeeping operation is not party to an armed conflict. It will not, however, cover collective and organized acts of defending civilians by a CPKO's military unit. Such acts may give rise to an armed conflict or be part of the hostilities if an armed conflict already exists, as explained in Section III.A.

A critical question is whether the principle of impartiality makes the belligerent nexus criterion redundant. This is because acts that fall within the

72. *See also* Watkin, *Opportunity Lost*, *supra* note 69, at 641.

73. DPH GUIDANCE, *supra* note 26, at 54–55.

74. The United States takes a broader view to also include acts that "effectively and substantially contribute to an adversary's ability to conduct or sustain combat operations," *see* DOD LAW OF WAR MANUAL, *supra* note 27, § 5.9.3.

75. DPH GUIDANCE, *supra* note 26, at 58.

76. *Id.* at 61.

peacekeeping mandate should not be in support of any party to the conflict and should be executed in an impartial manner. One could say that only acts that fall outside the peacekeeping mandate could possibly meet this test. However, whether there is support or detriment is a factual question. As the ICRC *Interpretive Guidance* states, what matters is the objective purpose of the act.[77] Consequently, any act by a civilian cyber peacekeeper that objectively harms a party to the armed conflict, for example by destroying its networks, will satisfy the belligerent nexus test regardless of whether the cyber peacekeepers acted impartially or did not intend to disadvantage a particular party.

An issue that can cause difficulties in applying DPH to cyber peacekeeping is the timeframe within which those committing DPH can be lawfully targeted. The time frame spans from preparatory acts, the deployment phase, and the act itself, up to the actor's disengagement and return.[78] Apparently, the DPH timeline is quite narrow if the speed with which cyber operations are carried out is taken into account. For example, when does disengagement from cyber-attacks occur? Is it immediately after the individual presses the button? In cyber operations, the act and the disengagement may happen simultaneously. Even if an integrated approach is taken to cyber operations, it will still be difficult to satisfy the DPH timeline because it is difficult to decipher operations and operations may happen simultaneously.

We thus conclude by stating that unless the DPH formula is adapted to suit cyber operations, its application to CPKO will be limited.

IV. THE USE OF LETHAL FORCE ACCORDING TO THE LAW ENFORCEMENT PARADIGM

The law enforcement paradigm is governed by IHRL and, more specifically, by the norms regulating the right to life. It will primarily apply to cyber peacekeepers' use of lethal force in self-defence or defence of others outside an armed conflict situation[79] but it will also apply within an armed conflict context when the CPKO does not become a party thereto. The law enforcement

77. *Id.* at 59.

78. *Id.* at 65–68. For criticism see Boothby, *supra* note 69; Michael N. Schmitt, *The Status of Opposition Fighters in a Non-International Armed Conflict*, 88 INTERNATIONAL LAW STUDIES 119, 136 (2012). *See also* DOD LAW OF WAR MANUAL, *supra* note 27, § 5.8.4.

79. The Security Council, for example, frequently authorizes peacekeepers to use force "within their capabilities" to protect civilians "under imminent threat of physical violence." *See, e.g.*, S.C. Res. 1265 (1999); S.C. Res. 1296 (2000); S.C. Res. 1267 (2006); S.C. Res. 1894

paradigm will also apply in situations of armed conflict to the defensive use of lethal force by the CPKO's civilian personnel, such as its police personnel, provided that the use of force does not amount to direct participation in hostilities, for example by defending combatants against attacks within the meaning of IHL. The law enforcement paradigm will apply in this case even if the military contingent of a CPKO becomes a party to the armed conflict. IHRL will also apply to situations where soldiers exercise their right to personal self-defence against lethal attacks outside an armed conflict situation or during an armed conflict, provided that their right to self-defence in the latter case has not been limited by the commander and does not amount to participation in the armed conflict.[80] Finally, IHRL will apply to situations of armed conflict, in particular NIACs, when the CPKO, including its military personnel, engages with rioters, demonstrators, or others not committing DPH, or is involved in other law enforcement operations which are not linked to the armed conflict.[81]

Having explained the situations where the law enforcement paradigm applies, in the sections that follow we will establish whether IHRL applies extraterritorially where CPKO are deployed and the extent to which a CPKO is bound by IHRL. We will then consider how the use of lethal force is regulated by IHRL and, more specifically, the right to life.

(2009) (on the protection of civilians in armed conflict). *See also* Nicholas Tsagourias, *Self-Defence, Protection of Humanitarian Values, and the Doctrine of Impartiality and Neutrality in Enforcement Mandates*, *in* THE HANDBOOK ON THE USE OF FORCE IN INTERNATIONAL LAW 398–415 (Marc Weller ed., 2015).

80. Prosecutor v. Sesay et al., Case No. SCSL-04-15-T, Trial Judgment, ¶ 1937 (Special Court for Sierra Leone Mar. 2, 2009); Prosecutor v. Sesay et al., Case No. SCSL-04-15-A, Appeals Chamber Judgment, ¶ 531 (Special Court for Sierra Leone Oct. 26, 2009) ("The Appeals Chamber notes that it is settled law that peacekeepers—like civilians—are entitled to use force in self-defence; such use does not constitute taking a direct part.").

81. Louise Doswald-Beck, *The Right to Life in Armed Conflict: Does International Humanitarian Law Provide all the Answers?*, 88 INTERNATIONAL REVIEW OF THE RED CROSS 881–904 (2006); DPH GUIDANCE, *supra* note 26, at 63; Basic Principles on the Use of Force and Firearms by Law Enforcement Officials, ¶ 1, https://www.ohchr.org/EN/ProfessionalInterest/Pages/UseOfForceAndFirearms.aspx (last visited Jan. 28, 2022) (adopted by the Eighth U.N. Congress on the Prevention of Crime and the Treatment of Offenders and welcomed by the U.N. General Assembly in G.A. Res. 45/166 (Dec. 18, 1990)) [hereinafter U.N. Basic Principles]; Güleç v. Turkey, App. Nos. 54, 1997, 838, 1044, Judgment, ¶¶ 72–73 (ECtHR July 27, 1998); McCann and Others v. United Kingdom, App. No. 18984/91, Judgment, [1995] ECHR 31 (Sept. 27).

A. The Applicability of IHRL to Cyber-Peacekeeping

In order to establish whether a CPKO is bound by IHRL, we need to establish whether the parent organization, in this case the UN, is bound by IHRL. Although the UN is not a party to human rights treaties, as an international organization with legal personality it is bound by IHRL as general principles of international law and/or customary law.[82] Consequently its CPKOs, as subsidiary organs of the UN, are bound by customary IHRL and, more specifically, by the right to life, which has acquired customary law status.[83] Troop contributing countries to a CPKO are bound by their treaty-based human rights obligations, but also by customary IHRL. Whether it is the UN's or the troop contributing country's human rights obligations that apply depends on the line of command and the particular circumstances surrounding the impugned act. We start from the assumption that the UN's IHRL obligations will in principle apply to peacekeeping operations under its command and control.

That having been said, it is true that the applicability of IHRL is concurrent with the exercise of jurisdiction.[84] Jurisdiction is attendant to sovereignty and has a strong territorial dimension. The question then is whether the UN as a non-sovereign entity with no territory of its own can actually exercise human rights jurisdiction. In order to answer this question, we need to look at the essence of jurisdiction and disentangle it from sovereignty and territory. Jurisdiction refers to authority and control, that is the power to regulate or effect persons, objects, or conduct. The UN can exercise such authority and control in the course of a CPKO, for example, it can detain or kill someone.

The next issue to consider is under what circumstances the UN's IHRL obligations apply extraterritorially to the extent that its CPKOs are deployed

---

82. Interpretation of the Agreement of 25 March 1951 between the WHO and Egypt, 1980 I.C.J. 89 (Dec. 20); Reparation for Injuries Suffered in the Service of the United Nations, Advisory Opinion, 1949 I.C.J. 174, 179 (Apr. 11).

83. *See, e.g.*, G.A. Res. 217 (III) A, Universal Declaration of Human Rights art. 3 (Dec. 10, 1948); International Covenant on Civil and Political Rights art. 6, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]; Convention for the Protection of Human Rights and Fundamental Freedoms art. 2, Nov. 4, 1950, 213 U.N.T.S. 222 [hereinafter ECHR]; American Convention on Human Rights art. 4, Nov. 22, 1969, 1144 U.N.T.S. 123; African Charter on Human and Peoples' Rights art. 4, June 27, 1981, *reprinted in* 21 INTERNATIONAL LEGAL MATERIALS 58 (1982).

84. *See, e.g.*, ICCPR, *supra* note 83, art. 2; ECHR, *supra* note 83, art. 1.

on the territory or within the jurisdiction of States.[85] In this respect, we shall apply by analogy the conditions developed in international jurisprudence on the extraterritorial application of human rights by noting that not only treaty, but also customary IHRL applies extraterritoriality, with the right to life being such a customary right.[86]

Turning now to the conditions according to which IHRL can apply extraterritorially, international jurisprudence has established two models: a spatial and a personal model.

According to the spatial model, human rights apply extraterritorially where there is effective control over territory through the deployment of forces or through a subordinate administration.[87] The spatial model can thus apply to a CPKO as part of a physical PKO which controls certain territory. For example, it will apply to situations where a peacekeeping force exercises governmental powers over a certain territory or exercises physical control over an area in order, for example, to perform disarmament and demilitarization activities or to enforce a buffer zone. It will also apply to a peacekeeping force which controls certain establishments, such as camps or detention centers.[88] In such situations, cyber peacekeepers are bound to respect the right to life of all persons within their area of authority and control. Whether

---

85. That human rights apply extraterritorially in the context of peacekeeping has been recognized by the UN Human Rights Committee, albeit in relation to States. U.N. Human Rights Committee, General Comment No. 31 [80], The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, ¶ 10, U.N. Doc. CCPR/C/21/Rev.1/Add. 13 (Mar. 29, 2004):

> This principle [to respect and ensure respect of the Convention] also applies to those within the power or effective control of the forces of a State Party acting outside its territory, regardless of the circumstances in which such power or effective control was obtained, such as forces constituting a national contingent of a State Party assigned to an international peace-keeping or peace-enforcement operation.

86. TALLINN MANUAL 2.0, *supra* note 34, r. 34, ¶ 7. We should mention, however, that the United States does not accept the extraterritorial application of IHRL. *See* U.N. Human Rights Comm., Concluding Observations on the Fourth Periodic Rep. of the United States, ¶ 22, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014); DOD LAW OF WAR MANUAL, *supra* note 27, § 1.6.3.3. *See also* Beth Van Schaack, *The United States' Position on the Extraterritorial Application of Human Rights Obligations: Now is the Time for Change*, 90 INTERNATIONAL LAW STUDIES 20 (2014).

87. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 109 (July 9); Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment 2005 I.C.J. 168, ¶ 168 (Dec. 19); Al Skeini v. United Kingdom, 2011-VI Eur. Ct. H.R. 99, ¶¶ 131–135, 138–140.

88. LEUVEN MANUAL, *supra* note 39, at 79–80.

the spatial model can apply to a purely online CPKO and to virtual control is very much doubted. For example, monitoring a network or data is too transient to establish the required threshold of authority and control envisaged by existing jurisprudence and, even if one could say that certain human rights such as the right to freedom of expression may apply in such cases, the level of authority and control is not sufficient to support the application of the right to life.

The personal model covers situations where authority and control are exercised over a person by a State agent or an agent of an international organization.[89] This model relies on physical control and would apply, for example, to persons who are under the authority and physical control of UN organs or persons within establishments under the authority and effective control of the UN, such as detention centers. Whether it can apply to the use of lethal force when no physical control over an individual exists is doubtful. For example, the European Court of Human Rights did not apply this model to air bombardment, holding that air bombardment does not establish control over the area where the bombs land.[90] It follows from this that the personal model will not apply to an online CPKO because there is no physical control over the targeted individual. It also will not apply to a physical peacekeeping operation which uses cyber (or kinetic) lethal force against individuals over whom it has no physical control or who are situated outside its area of spatial control. An example will be a cyber-attack by a cyber peacekeeper that kills a threat actor situated in a neighbouring State.

In an effort to close such gaps in human rights protection, it has been claimed that no territorial limitation should exist in relation to human rights, such as the right to life, that impose negative obligations.[91] According to this line of reasoning, what matters is the violation of the right to life by killing someone and the fact that there is control over the agent that uses lethal force. Another approach, which can be labelled as a "functional approach to

89. Al-Skeini v. United Kingdom, 2011-IV Eur. Ct. H.R. 99, ¶¶ 136–137.

90. Banković and Others v. Belgium, 2001 Eur. Ct. H.R. 333, ¶¶ 74–82. In *Al Skeini* the Court took a more nuanced approach without, however, specifying the conditions. *Al-Skeini*, 2011-IV Eur. Ct. H.R. 99, ¶ 136. In *Georgia v. Russia No. 2,* the European Court of Human Rights reverted to *Banković*. *See* Case of Georgia v. Russia (II), App. No. 38263/08, ¶¶ 132–36 (Jan. 21, 2021) (ECtHR), http://hudoc.echr.coe.int/eng?i=001-207757.

91. *See* MARCO MILANOVIC, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES: LAW, PRINCIPLES, AND POLICY 208–20 (2011); Helen McDermott, *Application of the International Human Rights Law Framework to Cyberspace*, *in* HUMAN RIGHTS AND 21ST CENTURY CHALLENGES 191, 203 (Dapo Akande et al. eds., 2020).

jurisdiction" and is based on the Human Rights Committee's General Comment 36, opines that the obligation to respect and ensure respect of the right to life covers "all persons over whose enjoyment of the right to life [the State] exercises power or effective control. This includes persons located outside any territory effectively controlled by the State, whose right to life is nonetheless impacted by its military or other activities in a direct and reasonably foreseeable manner."[92]

If the aforementioned approaches are adopted, it is theoretically possible to apply human rights extraterritorially to the use of lethal force by cyber peacekeepers. It remains to be seen, however, whether any of these approaches will be accepted by States but we can still voice our concerns.[93] Our main concern is that the aforementioned approaches globalize human rights jurisdiction whereby any State would be deemed to exercise jurisdiction over anyone anywhere in the world, in particular if the interconnected nature of cyberspace is taken into account. This not only runs roughshod over the exceptional character of the extraterritorial application of human rights but the jurisdictional, legal, and political difficulties it will cause are very serious. It should be noted in this respect that courts such as the European Court of Human Rights in the recent *Georgia v. Russia (II)* case seem to revert to physical control by rejecting the view that "anyone adversely affected by an act imputable to a Contracting State, wherever in the world that act may have been committed or its consequences felt, is thereby 'brought within' the 'jurisdiction' of that State for the purpose of Article 1 of the Convention."[94]

In conclusion we can say that, according to existing jurisprudence, the circumstances under which human rights obligations can apply extraterritorially in the context of a CPKO are quite limited.[95] With this caveat in mind, we will now proceed to discuss how the use of lethal force in self-defence or

92. U.N. Human Rights Committee, General Comment No. 36, Article 6: Right to Life, ¶ 63, U.N. Doc. CCPR/C/GC/36 (Oct. 30, 2018) [hereinafter General Comment No. 36]. *See also* Yuval Shany, *The Extraterritorial Application of Human Rights Law*, 409 COLLECTED COURSES OF THE HAGUE ACADEMY OF INTERNATIONAL LAW 88 (2020).

93. TALLINN MANUAL 2.0, *supra* note 34, r. 34, ¶¶ 8–10.

94. *Georgia v. Russia (II)*, App. No. 38263/08, ¶¶ 134–36 (citing *Banković and Others*, 2001 Eur. Ct. H.R. 333, at ¶ 75).

95. We will not discuss here the question of attribution which is a prerequisite for establishing responsibility for violations of the right to life. *See Al-Skeini*, 2011-IV Eur. Ct. H.R. 99, ¶ 135. For cyber attribution, see Nicholas Tsagourias & Michael Farrell, *Cyber Attribution: Technical and Legal Approaches and Challenges,* 31 EUROPEAN JOURNAL OF INTERNATIONAL LAW 941 (2021).

the defence of others can be regulated by the law enforcement paradigm and, more specifically, by the right to life.

B. The Use of Lethal Force and the Right to Life

In this section we will explain the customary law criteria justifying the lawful deprivation of life and apply them to the use of lethal force by cyber peacekeepers.

The protection of the right to life has been enshrined in many human rights instruments but its protection is not absolute. Article 6 of the International Covenant on Civil and Political Rights, for example, states that "no one shall be arbitrarily deprived of this right"[96] whereas Article 2 of the European Convention on Human Rights provides that no one shall be deprived of their life intentionally, except "when it results from the use of force which is no more than absolutely necessary: (a) in defence of any person from unlawful violence; (b) in order to effect a lawful arrest or to prevent the escape of a person lawfully detained."[97] According to Article 3 of the Code of Conduct for Law Enforcement Officials, "law enforcement officials may use force only when strictly necessary and to the extent required for the performance of their duty."[98] The UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials states:

> Law enforcement officials shall not use firearms against persons except in self-defence or defence of others against the imminent threat of death or serious injury, to prevent the perpetration of a particularly serious crime involving grave threat to life, to arrest a person presenting such a danger and resisting their authority, or to prevent his or her escape, and only when less extreme means are insufficient to achieve these objectives. In any event, intentional lethal use of firearms may only be made when strictly unavoidable in order to protect life.[99]

What transpires from the aforementioned provisions is that life should not be taken arbitrarily. A non-arbitrary and therefore lawful deprivation of

96. ICCPR, *supra* note 83, art. 6.

97. ECHR, *supra* note 83, art. 2.

98. G.A. Res. 34/169, U.N. Code of Conduct for Law Enforcement Officials (Dec. 17, 1979).

99. U.N. Basic Principles, *supra note* 81, ¶ 9. This principle constitutes customary law. *See* Interim Report of the Special Rapporteur Philip Alston on Extrajudicial, Summary or Arbitrary Executions, ¶ 35, U.N. Doc. A/61/311 (Sept. 5, 2006).

life should, according to established jurisprudence, meet three conditions: necessity, proportionality, and precautions.[100] These are customary law conditions which will also apply to the use of lethal force by cyber peacekeepers.

According to the first condition, that of necessity, the use of lethal force to defend peacekeepers or others from imminent death or serious injury should be the only available option because all other non-lethal alternatives (such as arresting the suspect) have been exhausted, are ineffective, or too risky.[101] Moreover, the threat should be present when force is used, thus excluding past threats. It should be noted, however, that necessity does not require "equality of arms;" lethal force through cyber means can be used to defend against cyber or physical threats to life. Furthermore, force should be used "as gradually as possible," although that does not mean that lethal force cannot be used immediately if the circumstances so require.[102] A critical question is how the necessity of the use of lethal force can be assessed. The better view is to assess necessity from the perspective of a reasonable peacekeeper in light of the circumstances prevailing at the time and the information available to him or her. In other words, the assessment of necessity should be based on a reasonable *ex-ante* standard.[103] This is a critical issue in the context of CPKO because the particular features of cyber operations often require quick decisions in situations of factual uncertainty.

The second condition, proportionality, requires that the use of lethal force must be proportionate to the risk it addresses.[104] Such assessment can

---

100. General Comment No. 36, *supra* note 92. In addition to these three requirements, the right to life imposes further obligations before or after the use of force, such as conducting an independent investigation.

101. U.N. Code of Conduct for Law Enforcement Officials, *supra* note 98, art. 3(c); U.N. Basic Principles, *supra* note 81, ¶ 4. *See also* Report of Special Rapporteur Christof Heyns on Extrajudicial, Summary or Arbitrary Executions, ¶ 59, U.N. Doc A/HRC/26/36 (Apr. 1, 2014) (on the different components of the necessity test).

102. U.N. DEP'T OF PEACE OPERATIONS, THE PROTECTION OF CIVILIANS IN UNITED NATIONS PEACEKEEPING HANDBOOK ¶ 12.4 (2020); U.N. Dep't of Peacekeeping Operations, Use of Force by Military Components in United Nations Peacekeeping Operations, ¶¶ 11–12 (Jan. 2017); Report of Special Rapporteur Christof Heyns on Extrajudicial, Summary or Arbitrary Executions, *supra* note 101, ¶ 61.

103. McCann and Others v. United Kingdom, App. No. 18984/91, Judgment, [1995] ECHR 31, ¶ 135 (Sept. 27); Güleç v. Turkey, App. Nos. 54, 1997, 838, 1044, Judgment, ¶ 71 (ECtHR July 27, 1998); Aydan v. Turkey, App. No. 16281/10, Judgment, ¶¶ 97–99 (ECtHR June 12, 2013).

104. U.N. Basic Principles, *supra* note 81, ¶ 5; U.N. Code of Conduct for Law Enforcement Officials, *supra* note 98, art. 3(b); Report of Special Rapporteur Christof Heyns on Extrajudicial, Summary or Arbitrary Executions, *supra* note 101, ¶¶ 65–73.

be made on a case-by-case basis.[105] It can factor in the intensity, extent, and probability of harm as well as any threat to innocent bystanders. Even if the cyber peacekeeper knows that innocent civilians may be killed, whether the use of lethal force will still be proportionate can be assessed against the fact that innocent civilians may have been killed in any case by the initial act or that their death may save more lives. For example, if a person inserts a logic bomb into a system and threatens to activate it to cause deaths, targeting that person and incidentally killing his or her collaborators will be proportionate if more lives that otherwise would have perished by the explosion are saved.

Finally, the duty to take feasible precautions acts as a logical corollary to necessity and proportionality. It places an obligation on the UN to train its cyber peacekeepers appropriately, which in this case would also include technical training. It also places an obligation to plan cyber operations and exercise such command and control as to minimize risks to life or limb.[106] The UN, for example, is complying with this obligation by publishing guidelines on the use of lethal force and specifying them in the rules of engagement.[107]

In what follows we will discuss multiple scenarios illustrating how IHRL can apply to the use of lethal force in the context of CPKO.

The first scenario involves a civilian police unit of a CPKO that is tasked with monitoring and protecting the networks of the host State's water treatment facility, which is part of its critical national infrastructure. The police unit becomes aware that a hacker is planning to launch a cyber-attack against the facility's software program. If successful, the water will be poisoned, endangering the life of a large portion of the population. In order to determine whether the use of lethal force would be lawful in this instance, the threat to civilian life must be imminent. In order to establish imminence, the available information (for example, intercepted messages) should signal a concrete intention to do so and indicate capacity to mount the cyber-attack. Once imminence is established, the cyber peacekeeping unit should exhaust all non-lethal means to prevent the cyber-attack. For example, it can use active cyber defence measures aimed at stopping the cyber-attack by incapacitating or destroying the attacker's servers. These operations should, however, comply with the criterion of proportionality by not disproportionately affecting

105. U.N. Basic Principles, *supra* note 81, ¶ 5(a).

106. McCann and Others v. United Kingdom, App. No. 18984/91, Judgment, [1995] ECHR 31, ¶¶ 203–10 (Sept. 27).

107. U.N. Basic Principles, *supra* note 81; ALAN COLE ET AL., SANREMO HANDBOOK ON RULES OF ENGAGEMENT (2009).

other networks or lead to death or injury of innocent civilians. Cyber peacekeepers may also try to negotiate and persuade the attacker to suspend the attack. However, if non-lethal means—cyber or non-cyber—are infeasible or ineffective, resort to lethal force (kinetic or cyber) would satisfy the requirement of necessity and, in this scenario, would also comply with the condition of proportionality, since lethal force would not exceed the objective of protecting the life of civilians threatened from the cyber-attack. The obligation to take precautions would also require cyber peacekeepers to minimize the effects of lethal force in the planning phase of the cyber operation, for example by avoiding disrupting the functionality of civilian networks.

Conversely, consider a scenario where a hacker launches a ransomware attack by blocking access to the computer networks of a hospital monitored by a cyber peacekeeping unit and demanding a monetary payment in order to regain control. In this case, the use of lethal force against the hacker will be lawful if there is an imminent threat to life. If, for instance, the computer systems contain medical records of patients that need urgent, life-saving medical care, a case can be made that failure to access those medical records represents a threat to the patients' lives. If the information stored within the locked computer systems is of an administrative nature, there would be no imminent threat to life. Would the use of lethal force still be necessary? We think that in such circumstances it would not be necessary because other means could be used to unlock the system. The use of lethal force will not unlock the system and protect civilian lives. It would also be unlawful to use lethal force against the hacker in order to compel his or her accomplices to unlock the system.

Another scenario concerns the use of lethal force to effectuate arrests[108] in a context where peacekeepers are mandated to apprehend criminal gangs, as in the Operation Sukula conducted by the Multidimensional Integrated Stabilization Mission in the Central African Republic.[109] Suppose that dangerous members of a criminal gang responsible for many killings escape ar-

108. *See* ECHR, *supra* note 83, art. 2(2)(b).

109. Letter Dated 23 July 2018 from the Panel of Experts on the Central African Republic Extended Pursuant to Resolution 2399 (2018) Addressed to the President of the Security Council, U.N. Doc. S/2018/729 (July 23, 2018); Security Council Press Statement on Attack against United Nations Multidimensional Integrated Stabilization Mission in Central African Republic, U.N. Doc. SC/13291-PKO/724 (Apr. 11, 2018). The UN Multidimensional Integrated Stabilization Mission in the Central African Republic is mandated to "arrest and detain in order to maintain basic law and order." *See* S.C. Res. 2552 (Nov. 12, 2020).

rest by hijacking a self-driving car. They also threaten to kill the car's passengers if arrested. A cyber peacekeeper manages to interfere with the car's computerized system with a view of arresting them by stopping the car but, instead, causes an accident which leads to the death of the gang members and the car's passengers. In this case the gang members pose a clear and imminent danger to the life of others and possibly immediate danger to the life of peacekeepers. Their death was not however deliberate but was caused by the cyber peacekeeper's action to interfere with the car's system. This is a case of potential use of lethal force to effectuate an arrest.[110] In such circumstances, the deaths would be lawful, provided that they were necessary (all non-lethal alternatives were employed to no avail or would have proven ineffective) and proportionate. Even if the use of lethal force was deliberate, it would still be lawful to the extent that non-lethal alternatives did not exist and the deaths were proportionate.[111]

A question that can be asked regarding the law enforcement paradigm is whether lethal force can be used to defend peacekeeping material or objects, for example computers or networks. National laws differ regarding the use of lethal force to defend property and one can say that material, objects, and installations are not a peacekeeper's property as property is defined in national law. However, it seems that, according to UN conventions and guidelines, computer systems and networks may indeed fall within the category of property. This can be deduced, inter alia, from Article 7 of the 1994 Convention on the Safety of UN Personnel, which protects "United Nations and associated personnel, their equipment and premises" from attack or from any action preventing them from discharging their mandate.[112] Also, according to the 2003 *Handbook on United Nations Multidimensional Peacekeeping Operations,* self-defence includes the "right to protect oneself, other UN personnel, UN property and other persons under UN protection."[113] Furthermore,

110. DAVID J. HARRIS ET AL., LAW OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 232 (3d ed. 2014); Louise Doswald-Beck, *The Right to Life in Armed Conflict: Does International Humanitarian Law Provide all the Answers?*, 88 INTERNATIONAL REVIEW OF THE RED CROSS 881, 886 (2006); U.N. Basic Principles, *supra* note 99, ¶ 9.

111. KENNETH WATKIN, FIGHTING AT THE LEGAL BOUNDARIES: CONTROLLING THE USE OF FORCE IN CONTEMPORARY CONFLICT chaps. 11–13 (2016); SEUMAS MILLER, SHOOTING TO KILL: THE ETHICS OF POLICE AND MILITARY USE OF LETHAL FORCE (2016).

112. Convention on the Safety of the United Nations and Associated Personnel art. 7, Dec. 15, 1994, 2051 U.N.T.S. 363.

113. U.N. DEPARTMENT OF PEACEKEEPING OPERATIONS, HANDBOOK ON UNITED NATIONS MULTIDIMENSIONAL PEACEKEEPING OPERATIONS 57 (2003).

according to the Statute of the International Criminal Court, it is a war crime to attack peacekeeping personnel, material, installations, or vehicles if they are entitled to civilian protection. This rule applies to IACs as well as to NIACs.[114]

In light of the above, it can be said that lethal force can be used to protect cyber peacekeepers' property, such as their computers, from attack if the attack poses a risk to their life, provided, of course, that the other criteria are met. In such cases, the ultimate object of protection is life even if in doing so the property is also protected. Can, however, peacekeeping property, such as computers, be protected through the use of lethal force even if safeguarding life is not the ultimate object of protection? One could say that peacekeeping objects are of a particular value and therefore lethal force can be used to protect them if it is necessary, proportionate, and precautions are taken. In support of this view, Article 31(1)(c) of the Statute of the International Criminal Court should be mentioned, which excludes criminal responsibility if a person defends property essential for the accomplishment of a military mission. Although the article refers to criminal responsibility and military missions, one can apply its spirit to the case at hand.

V. CONCLUSION

In this article we introduced the concept of cyber peacekeeping and discussed the problems that arise regarding the use of lethal force, distinguishing between the law of armed conflict paradigm and the law enforcement paradigm. In relation to the law of armed conflict paradigm, we explained the conditions of applicability of IHL and when cyber peacekeeping forces become a party to an IAC or NIAC. Further, we explained when they become combatants, remain civilians, or take direct part in hostilities.

In relation to the law enforcement paradigm, we discussed the general issue of the applicability of human rights law to cyber peacekeeping as well as the circumstances under which IHRL applies extraterritorially. We then considered how the criteria of necessity, proportionality, and precautions that regulate the lawful deprivation of life apply to the use of lethal force in the course of peacekeeping by discussing various scenarios.

As a final remark we should say that this article is one of the first to provide a systematic study of how the existing IHL and IHRL regimes apply

114. Rome Statute of the International Criminal Court arts. 8(2)(b)(iii), 8(2)(e)(iii), July 17, 1998, 2187 U.N.T.S. 90.

to cyber peacekeeping and, in particular, to the use of lethal force. The article indicated that applying the aforementioned regimes encounters two sets of difficulties. The first relates to the uncertainty surrounding their application to peacekeeping in general. The second refers to the particular challenges posed to IHL and IHRL by cyber peacekeeping. The article addressed some of the difficulties and provided, where possible, solutions that can also apply to peacekeeping in general.