Cyber Challenges vis-à-vis Peace Operations

United Nations Digital Blue Helmets: the Beginning of Cyber Peace Keeping?

A cura di Annachiara Rotondo

For over a decade cyberspace has turned into a theatre for aggressive operations, alternative and complementary to the classical land maritime and aerial military operations, and cyber tools have begun to play a significant role in terms of achievement of strategic advantages (e.g. in terms of acquisition of information) to the point that "many ongoing situations of crisis, both below and above the level of armed conflict, have attracted a significant and persistent cyber component".[1] Recent practice showed, in fact, that several conflicts and crisis of twenty-first century contained a significant cyber element, as in the case of the dispute between India and Pakistan over Kashmir, Arab Spring or Syrian conflict.[2] Hence, it seems worth reflecting, in terms of international law, on ICT's impact on peace operations aimed at facing threats to the peace, breaches of the peace or acts of aggression, whatever their nature.

[1] KLEFFNER J. K., HARRISON DINNISS H. A., *Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations*, 89, Int'l. L. Stud. Ser. US Naval War, Vol. 89, 2013, p. 512. [2] *Ibid*, p. 512, 513.

Contemporary peace operations stand out for having a multilateral character embracing numerous tasks as the maintenance of internal public order, the promotion of a stable environment and the

ISSN 2531-6931

protection of civilians' human rights.[2] And considering the amount of activities governments and people have moved into cyberspace and that the latter works as a complementary dimension to States' land, sea and air space,[3] it seems - at least plausible – to support the idea of future peace operations including cyber activities: i.e. the so-called 'cyber peace keeping'. Among scholars is slowly becoming a common understanding that cyberspace must be included among peacekeepers' fields of action because ICT can represent an efficient tool to exacerbate internal crisis and conflicts, acting towards cyber threats against the State's stability and, more broadly, giving a general support to peacekeepers' activities.

Recently, cyber peace keeping has been defined as "actions(s) undertaken in cyberspace to preserve peace, however fragile, where fighting has been halted and to assist in implementing agreements achieved by the peacemakers".[4]

However, nowadays that peace keeping acquired a multifunctional character, this definition appears rather reductive. Indeed, besides the typical functions carried out by peace keepers - as the implementation of ceasefire agreements - current cyber peace keeping can be finalized to the achievement of additional goals before, during or after a conflict. For instance, in post-conflict situations cyber operations can deflate internal crises, targeting social media inciting violence against local (ethnic, religious, political) groups, reducing the appeal of extremists' fringes on the media and contrasting their recruitment activities in the deep web.

More specifically, according to some scholars, cyber peace keeping pursues six main objectives in all the stages of a crisis: the protection of civilians, the increasing of trust and security in cyberspace, the

---

[2] *Ibid*, p. 515.

[3] Indeed, it is not by chance that among scholars some labelled cyberspace as "the new global common". *Inter alia* T. MURPHY, *Security Challenges in the 21st Century Global Commons*, in *Yale Journal of International Affairs*, Spring | Summer 2010; J. SHACKELFORD, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, in *Berkeley Journal of International Law*, 27, p.220, 2009.

[4] M. ROBINSON, K. JONES, H. JANICKE, L. MAGLARAS*, An Introduction to Cyber Peacekeeping,* 2018, p. 4, https://arxiv.org/pdf/1710.09616.pdf.

prevention of conflict escalation, the containment of conflicts especially with regard to damages to the detriment of population and

infrastructures, the aftermath containment and the rehabilitation of infrastructures, security and trust. [5]

Nevertheless, beyond the literature the concept of cyber peace keeping remains purely theoretical not having been so far formally adopted by States or international organizations. Indeed, mandates of contemporary peace operations do not refer to cyber-problems, avoiding envisaging topics as the defence of cyberspace, the detection of cyber threats or the protection of digital rights during conflicts or crisis situations. [6] Consequently, it seems worth reflecting on their legitimacy according to international law.

On the basis of an interpretation of the current legal framework of peace operations, it seems primarily correct to sustain the lawfulness of cyber operations conducted within the scope of the mandate, which are implemented with the consent of the territorial State with impartiality and, in case of cyber operations reaching the level of armed force, only of those designed to the purpose of self-defence.[7] On the contrary, cyber operations conducted outside "the scope of the host State's consent", or expressly prohibited by the further have to be labelled as impermissible. [8] Concerning peace operations employing the use of force, it seems reasonable to allow the employment of ICT when they consist in a mere support to the kinetic technologies, as those working to pinpoint a target. Instead, a cyber operation which is a forceful

[5] AKATYEV N., JAMES J. I., *Legislative Requirements for Cyber Peacekeeping*, Journal of Digital Forensics, Security and Law, Vol. 17, N. 13, 2017, p. 25.

[6] *Ibid*, p. 31.

[7] SCHMITT M., VIHUL L. (Eds.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, pp. 363, 364.

[8] *Ibid*, p. 364.

measure in itself - because of its effects - is generally to be considered as unlawful except for self-defence purposes.[9] Obviously, in the absence of practice, these considerations remain purely theoretical and the 2016 "United Nations Digital Blue Helmets Programme" represents the solely worthy initiative on the ground. The latter, which has been considered as the starting point for a "UN cyber peace keeping approach"[10], has been created to provide a common platform for United Nations' members, agencies and organs to share

ISSN 2531-6931

essential information for a better coordination of protective and defensive measures to combat dangerous cyber incidents. Generally, the Programme shares some of its main goals with most of the contemporary peace operations, focusing on the maintenance of international peace and security, the protection of human rights and the delivery of humanitarian aids.[11] Specifically, it deals with those critical cyber security components of Sustainable Development Goals such as: cyber-attacks on food chains as a potential threat for the achievement of the zero-hunger goal; cyber bulling and online exploitation of children in the context of goal n. 4 on quality education and also cyber-attacks on critical infrastructures.

In reaching its purposes Digital Blue Helmets Programme pursues long term strategies, some with a precautionary and defensive character such as the mitigation of "zero-day vulnerabilities", the enrichment of national cyber-security capabilities of UN Member States or the encouragement of better encryption to safe data, some others more active and offensive as the creation of cyber-security ground rules and the fight against on line trafficking.[12] The armed wing of the Programme is made of an elite team of experts capable of understanding risks and issues related to cyber-security supported by academia, cyber-security organizations, NGOs, think tanks and other relevant stakeholders in the field of cyber-security. Specifically, they are trained and knowledgeable practitioners, specialized in "event

[9] UN Doc. A/57/767, *Comprehensive review of the whole question of peacekeeping operations in all their aspects*, Mr. Alaa Issa, Report of the Special Committee on Peacekeeping Operations, 29 March 2003, § 46.

[10] AKATYEV N., JAMES J. I., *United Nations Digital Blue Helmets as a Starting Point for Cyber Peacekeeping*, 2017, https://arxiv.org/ftp/arxiv/papers/1711/1711.04502.pdf.

[11] UN Office of Information and Communication Technologies, *Digital Blue Helmets. Awareness. Protection. Security*, 2018, p. 22.

[12] *Ibid*, p. 18.

monitoring, operations, environment testing, digital forensics, and cyber audit and assessment".[13]

The creation of UN Digital Blue Helmet Programme demonstrates the necessity to introduce cyber components to peace operations but an international framework agreement and a common taxonomy on "cyber legal issues" are the necessary preliminary requirements to the development of a structured cyber peace keeping. [14] While terminological problems may induces to substantial misunderstandings (for instance the possibility of considering *a priori*

some cyber-attacks as veritable armed attacks) the lack of law would have the result of paralyzing peace keepers, assailed by the doubt that any operative choice within the cyberspace may lead to a violation of international law.

[13] *Ibid*, p. 4.

[14] AKATYEV N., JAMES J. I., *Legislative Requirements for Cyber Peacekeeping*, *cit.*, p. 28.