Establishment of UN Cyber Peacekeeping Force: Prospects and Challenges

NUST Journal of International Peace & Stability
2019, Vol. II (2) Pages 17-31
njips.nust.edu.pk

Fahad Nabeel [1]

Abstract

With the emergence of cyberspace as the fifth domain of warfare, the prospects of cyber conflicts have increased significantly. Around 300 state-sponsored cyber operations have been conducted since 2005. The future uncertainty of cyber-warfare has prompted calls for necessary measures to regulate the actions of states in cyberspace. In this regard, cyber-peacekeeping has also emerged as a significant research area to distinctively deal with the cyber component of future conflicts. Although, a number of challenges exist regarding materialization of full fledge cyber-peacekeeping force, it can be easily integrated into the current United Nations (UN) peacekeeping organizational structure. In legal terms, operationalization of cyber-peacekeeping *force* will depend on the mandate of peace operations approved by the UN Security Council (UNSC). This paper discusses the challenges confronting the creation of a cyber-peacekeeping force and also offers recommendations by presenting a general framework regarding how such a force can be operationalized. Despite the fact that a dedicated cyber-peacekeeping force seems a far sighted idea in present times, a distinct cyber unit can certainly be formed and integrated into UN peace operations in near future.

Keywords

Cyber-peacekeeping, cyber-security, cyber-warfare, United Nations, UN Peacekeeping

Introduction

For over a period of decade, cyberspace has evolved as the fifth domain of warfare. The weaponization of cyberspace in recent years has emerged as a key tool in transforming the nature of inter-state hostility. The United States (US) was responsible for pre-emptively cutting off Iraqi computer networks and internet grid before its invasion of the country in March, 2003 (e.g., Nabeel, 2019). Similarly, clear instances of the use of cyberspace as an arena for war were evident when Russia-based hackers were involved in deploying of cyber-attacks against Estonia in April, 2007 and Georgia in 2008. These incidents were regarded by several experts as the first events in history whereby cyber-warfare coincided with actual military action(s) (Markoff, 2008).

In the Middle East, Israel hacked into Syrian air defense systems in September, 2007 to blind the latter while Israeli jets were involved in the bombing of a suspected nuclear site in Diaya-al-Sahar. Under Obama administration, a joint US-Israel cyber-attack was launched, known as 'Operation Olympic Games', in which

[1] *Fahad Nabeel* works as a Senior Research Associate at Centre for Strategic and Contemporary Research (CSCR), Islamabad.
E-mail: fahad.n@cscr.pk

Stuxent, a sophisticated malware, was employed to temporarily shut down Iranian nuclear facility at Natanz. Similarly, in order to sabotage test launches of North Korean missile program, President Obama ordered cyber-attacks against North Korea in early 2014 (Nabeel,2019). David Sanger (2018) in his book claimed that at least 200 state-on-state cyber-attacks had been carried out by early 2018. However, the 'Council on Foreign Relations' Cyber Operations Tracker' documented at least 313 publicly known state-sponsored incidents which had occurred since 2005. With the increasing trend of cyber-attacks, scholars remain skeptic about the breakout of a cyber conflicts. The probability of cyber conflicts is meant to increase given the pace of states in equipping themselves with offensive and defensive cyber capabilities. Currently, more than 30 states have the capability to launch cyber-attacks.

Due to rising future uncertainty of cyber weapons and how they might impact the international security landscape, there has been an increasing demand for an *International-Level Cyber-Security Regime* which can regulate the activities of states in the realm of cyberspace. A number of proposals have been put forward in the past few years in this regard. One such proposal is that of establishing a United Nations (UN) cyber-peacekeeping force. Earliest researches on the subject of cyber-peacekeeping can be traced to at least July, 2002. At that time, Thomas P. Cahill, Konstantin Rozinov and Christopher Mule identified cyber-peacekeeping as a significant future research area. By examining the existing UN peacekeeping principles, the three scholars proposed as to how the peacekeeping principles can be applied in the cyber domain (Cahill, Rozinov, & Mule, 2003).

Considering the increasing tendency of conflict and crisis situation with a cyber-component and the deployment of complex peace operations, Kleffner and Dinniss (2013) raised the possibility that in near future, peacekeepers will find themselves in missions where they will encounter cyber incidents during, following or even in the absence of conventional hostilities. Their futuristic assumption was based on the rapidly accelerating weaponization of cyberspace in the past few years as a part of inter-state hostility. While raising the possibility of cyber component in future peacekeeping operations, Kleffner and Harrison believed that the future inclusion of cyber component in UN peacekeeping operation will largely depend on the type of operation and its constituting mandate.

The primary focus of this research is hence, to examine the prospects and challenges of establishing a UN cyber-peacekeeping force. In addition, challenges towards establishment of a peacekeeping force are addressed and recommendations are provided in this regard. Thereafter, conceptualization of cyber-peacekeepers in peace operations is analyzed through a legal framework. To the end, the initiatives taken by the UN regarding cyber-peacekeeping and a model framework is presented in order to explicate *how* the UN should proceed in future when considering the establishment of a cyber-peacekeeping force.

Defining Cyber-peacekeeping

In simple words, cyber-peacekeeping is analogous to physical peacekeeping. But unlike physical space, cyber-peacekeepers are deployed singularly for cyberspace alone. Robinson and colleagues (2018) define cyber-peacekeeping as;'The application of cyber capability to preserve peace, however fragile, where fighting has been halted and to assist in implementing agreements achieved by the peacemakers.'

They further argue that cyber-peacekeeper is an *'individual performing cyber peacekeeping activities'* (p. 5). Various scholars and experts have explained the potential roles of cyber peacekeepers. For instance, Phneah (2012) explains the role of

cyber-peacekeepers as; 'To define, observe and legislate to maximum compliance, and provide regulatory recommendations to improve existing laws to curb and minimize breaches.'

Contrarily, Kleffner and Dinniss (2013) explain that cyber-peacekeepers should the ability to 'prepare the battle space, neutralize networks and uncover and obtain documentary evidence will be useful tools in carrying out particular operations […]". On the other hand, Dorn (2017) elaborates in detail cyber-peacekeepers "could investigate major cyber-attacks and hacking events. They could help contain conflict between nations (and potentially between other conflict parties as well), prevent escalation of cyberwars, and help catch global cybercriminals.' While keeping the above discussion in view, several major and critical tasks have been identified by scholars and experts for cyber-peacekeepers, which include;

- monitoring for actions in cyberspace that violate peace agreements;
- monitoring changes in network structures;
- cybersecurity dispositions and network traffic,
- monitoring human rights abuses occurring in cyberspace;
- verifying compliance with cyber terms;
- creation of a cyber buffer zone[2];
- disarmament of cyber weapons;
- demobilization of cyber combatants;
- reintegrating of cyber ex-combatants towards sustainable livelihoods;
- reforming cyber aspects of security sector;
- offering electoral assistance by providing protection against hard and soft cyber-attacks;
- provision of malware education and coordinating emergency malware response teams;
- ensuring cyber-peacekeeping activities do not violate human rights
- promotion of human rights in cyberspace;
- bringing value to the restoration and extension of state authority only if state cyber dependence is moderate or high;
- monitoring the vague 'digital borders/boundaries';
- prevention or warning of impending cyber- attacks;
- investigating cyber-attacks;
- mediating between conflicting parties by either finding acceptable terms for 'cyber ceasefires' or developing 'cyber-peace agreements' for ending cyber conflicts;
- overseeing safe layers for netizens (Internet users) for cyberspace freed from viruses and attackers;
- overseeing 'safe areas' (secure, well-guarded servers or domains),

[2] Robinson et al., define cyber buffer zone as 'a network or site that is protected and monitored by peacekeeping forces, where cyber attacks have been excluded.'

- offering software fixes to parties affected by ransom-ware or website attacks;
- removing dormant malicious software activated by unwitting users or cyber weapons;
- assisting with national cyber infrastructure development;
- educating national cyber officials;
- bringing more order to weakly governed global cyberspace by promoting regulation of states activity;
- assisting the establishment of a new cyber norms and international cyber agreements.

Challenges

Experts on cyberspace and its usage as a potential arena for war opine that raising a virtual peacekeeping force is more challenging. Thus there have been major criticism on the very idea of establishing the force. The concerns, objections and criticisms are discussed in the following sections. The discussion will also contain recommendations as to how to overcome these challenges.

Insufficient Capabilities, Expertise and the Role of Cyber-Powers

Currently, the UN does not have sufficient capabilities and expertise to deploy a cyber-peacekeeping force. In-depth knowledge of sophisticated viruses, spear phishing schemes, the 'dark web' and national cyber-warfare capabilities are key components which will be required for creating a cyber-peacekeeping force. However, it is important to acknowledge that the UN lacks these components. At present, in order to overcome this gap, states should ensure the provision of necessary capabilities and expertise to their cyber experts. However, transferring of capabilities and expertise by states might prove challenging as states grapple with the question of impartiality or adopting narrow minded thinking under the disguise of national interests. In addition, states are themselves in need of cyber-experts. It is already estimated that there will be 3.5 million vacant cybersecurity roles, in future. Nevertheless, in the longer run, an international cybersecurity regime will be needed in order to regulate the growing activities of states in the cyberspace (Dorn, 2017).

Although cyber-peacekeeping was identified as a future research area nearly two decades ago, but the concept still remains rather nascent. A brief review of exiting literature on the phenomenon of 'cyber-peacekeeping' reveals a limited ongoing debate. (Consequently), some scholars believe that cyber-peacekeeping is still a new concept and need some time to be developed before being completely operationalized (e.g., Dorn, 2017). The main reason why major cyber powers including the United States, China and Russia would not endorse the creation of a UN cyber-peacekeeping force, is mainly because of security and confidentiality concerns and related issues. Nevertheless, Dorn (2017) believes that few states might allow for UN-led investigation of cyber-attacks on case-by-case basis where they emerge as vindicated (Dorn, 2017).

Redundant Measure

Some experts are of the opinion that establishing a cyber-peacekeeping force will be a redundant measure because existing peacekeeping mechanisms include efforts to deal with cyber-attacks in the form of inter-government cooperation to curb web breaches and will add to expenditures (e.g., Phneah, 2012). However, a review of recent international efforts undertaken to minimize cyber warfare threats have resulted in

certain measures. For instance, the UN Group of Governmental Experts (GGE) mechanism broke down following the disagreements on the new report regarding cyber norms in 2017. In November 2018, General Assembly passed two resolutions for establishing Russian-sponsored open-ended working group and the United States-sponsored GGE for regulating actions of states in the cyberspace. Experts believe that dividing the efforts for formulating norms into two groups will result in further complicating the already practiced international efforts for the formulation of cyber norms (Grigsby, 2018; Nabeel, 2019).

No Clarity of Physical or Visible Battlefield

The question of how the cyber-peacekeeping force will be able to distinguish physical or visible battlefield from the rest of cyberspace has garnered significant attention over the years and has been extensively debated upon by the experts on the subject (Dorn, 2017; Phneah, 2012). Unlike physical territorial boundaries, there are no territorial boundaries in cyberspace. Such argument should not prevent the establishment of cyber peacekeeping force because nature of cyber warfare is itself uncertain and not fully comprehended (Robinson et al., 2018).

Unavailability of Legal Framework

A number of legal issues have been raised and will continue to emerge in future regarding the conduct of cyber-peacekeeping force. As of present times there is no proper mechanism which can decide as to which cyber-attacks can be constituted as acts of war and otherwise (Phneah, 2012; Robinson et al., 2018). In case the threshold of armed conflict is crossed, the peacekeepers involved as part of the peace operation become a party to the armed conflict. This situation opens a number of challenges. First is the question of who will be party of the armed conflict? (i.e., troop-contributing state, or any responsible international organization like the UN, North Atlantic Treaty Organization, African Union or both). Second comes the concerns regarding the duration for which the peacekeepers remain party to armed conflict.

However, these legal hurdles can be resolved by addressing the aforementioned issues on case-by-case basis, while factoring in the operationalization of the mandate for the specific operation within the existing environment. In this regard, factors such as; relevant UNSC resolutions, specific operational mandates, adopted roles and practices by the peacekeepers, rules of engagement and operational orders, nature of armaments used by peacekeepers, interaction between the peacekeepers and conflicting parties, and conduct of the alleged victims and their fellow personnel, shall help in determining the nature of engagement for peacekeepers once the threshold of armed conflict is crossed.

International Law Perspective

From an international legal perspective, it is purview of the UNSC to decide whether cyber-operations (either in a specific situation or as a more general concept) amount to threating international peace and security under *Article 39* of the UN Charter which states that; 'The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security monitoring the vague 'digital borders/boundaries'(UN Charter Article 39).

However, when cyber operations are to be carried out in the context of peace operations under the threshold of an armed conflict, then such operations are also

subject to human rights law. In this regard, the UN General Assembly passed a historically unanimous *Resolution 68/167* which stated that the rights held by people offline must also be protected online. The Resolution also urged states to respect and protect the privacy in digital communication (Resolution/68/167, 2014).

The law of armed conflict can only be applicable for peace operations if the threshold of armed conflict is crossed. In other words, if cyber infrastructure or data is interfered with the objective to gather intelligence, preventing 'spoilers' from reigniting armed conflict or prevention of online postings reflecting racial hatred, it should be in accordance with human rights law provisions such as the right to privacy, freedom of expression, fear of association, etc. The mandate of peacekeeping varies from monitoring a peace agreement or ceasefire to protection of civilians, creating a safe and secure environment, while also training both civilians and armed forces (Kleffner & Dinniss, 2013). In this regard, the UNSC can also mandate non-forceful measures as a part of *Article 41* of the UN Charter for situations which it deems to as a threat to peace, breach of the peace or act of aggression. The *Article 41* states that (UN Charter Article 41); 'The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, (emphasis added by the author) and the severance of diplomatic relations.'

However, it is important to remain cognizant of the fact that not all cyber operations can be treated alike. The cyber operations which would amount to a use of force will not mandated by *Article 41*. Determination of whether a cyber operation amounts to a use of force or not, is explained in the following sub-section. In case individual members of a peace operation participated directly in hostilities will require a case-based assessment(s) to establish the required threshold of harms, causation and belligerent nexus. It will be fairly exceptional to think about the possibility of the operations in which peacekeepers and sole adversary are engaged in hostilities. Such a situation can arise only in case peacekeepers are deployed in an ongoing armed conflict and into a volatile situation that ultimately deteriorates, transforming into an armed conflict. In such operations, peacekeepers cannot conduct military operations, be it through cyber means or otherwise, because they are not subject to the law of armed conflict. As discussed earlier, conducting operations sanctioned by law of armed conflict require that peace operation is party to the armed conflict.

Meanwhile, law of occupation is applied to peace operations in certain circumstances, it does not imply that use of cyber operations by peace operation to project the execution of its mandate in those areas which are not under its physical control. In such a scenario, it will result in extending the applicability of the law of the occupation to those areas which have been targeted by cyber operations, for example for monitoring communications. This is because the use of cyber operation by occupying state to exercising her authority will not be sufficient on its own to establish an occupation. A territory is only considered to be occupied only when it is placed under the authority of the occupying force. The law of occupation is extended only to the territory were the authority of occupying force has been established and can be exercised (Kleffner & Dinniss, 2013).

Conceptualizing Deployment of Cyber Peacekeepers

Scenario A: Peacekeepers Deployed in a Region Marred by Offensive Cyber Operations

If peacekeepers are deployed in a situation where there are ongoing cyber operations between third parties, which can either be state-backed or non-state actors, then any response mechanism will depend on the mandate of the peace operation. However, it is imperative that peacekeepers will be authorized to monitor and conduct cyber operations in response to cyber threats. In this regard, any response will depend on four main factors;

- **(i)** mission's capabilities and resources;
- **(ii)** ensuring that response mechanism does not contravene; human rights law;
- **(iii)** robustness of the mandate;
- **(iv)** level of the cyber threat.

Considering a security situation which contains a cyber element, the UNSC sanctions a peace operation there without explicitly allowing the use of cyber operations for responding to incoming cyber threats, then the generic operational mandate will be interpreted broadly to include the monitoring of internet traffic in addition to monitoring of physical space. For monitoring of computer networks, there is need to first formulate a planning stage wherein cyber peacekeepers consult with local staff to build an overall picture of the networks, understanding the expected information to be flowing in and out and learn about any existing monitoring solutions (Robinson et al., 2019).

However, the permissible methods for monitoring internet traffic might differ. For example, all incoming and outgoing data traffic of mission's networks can be monitored as a matter of good network security. But the monitoring of data traffic of networks beyond the mission's own networks through technologies like Deep Packet Inspection (DPI)[3] will depend on whether the applicable law permits any such level of surveillance. However, conducting DPI will raise the issues related to privacy and freedom of expression (Kleffner & Dinniss, 2013). It is pertinent to mention here that right to privacy and freedom of expression are not absolute rights.

Article 19(3)(b) of International Covenant on Civil and Political Rights (ICCPR) states that certain interferences with the right of freedom of expression is permissible in case of protection of national security or of public order, or of public health or morals. But such exceptions are subject to proportionality requirements. On the other hand,

Article 17 of ICCPR which is related to right to privacy does not explicit mention reference to exceptions based on national security and public order but it allows for such exceptions conditional to the interference in an individual's privacy is neither arbitrary nor unlawful (International Covenant on Civil and Political Rights, 1966).

Therefore, while formulating mechanism for the use of DPI technology, it should be ensured that interference with rights given under human rights law is only for legitimate purposes. While considering the fact that troop contributing countries have different perspectives and approaches regarding the use of DPI technologies, it is

[3] The technology which allows looking into the content of the data packets that are used to transmit or receive information that is in the process of being transmitted.

important that rules related to permissible limits to the use of DPI and other Internet surveillance technologies should be clearly drafted.

In case of the applicability of law of armed conflict for a peace operation, the situation will alter drastically. Although human rights law will continue to be applied, the law of armed conflict permits the employment of those measures which are necessary for obtaining information about the enemy in order to meet required precautions in an attack. Such provisions of law of armed conflicts would prevail over the more generic conflicting rules of human rights law (Kleffner & Dinniss, 2013).

Scenario B: Offensive Cyber Operations Targeting UN Peace Operation

Since 2005, at least five cyber operations have been conducted against various UN entities, however, no publically known cyber-attack has been conducted against UN peace operations (Council on Foreign Relations, n.d.). While the possibility of future cyber-attacks against the peace operations cannot be ruled out completely, the UN peace operations should be prepared to chalk out mechanism to respond to cyber-attacks which either threaten the UN personnel or interfere in the implementation of peace operation's mandate. The principles of necessity and proportionality need to be factored in while formulating any response mechanism (Kleffner & Dinniss, 2013). The Just War Theory[4] is also a mechanism which can be utilized while formulating defensive mechanism against offensive cyber operations (Dorn, 2017). In case of a cyber-attack which either result in causing physical harm to UN personnel or cause loss of functionality by damaging property and equipment, use of force can be exercised for self-defense to such an extent that it complies with the principles of necessity and proportionality. The use of force will also be allowed in case a cyber-attack which obstructs the ability of a peace operation in performing its mission by compromising its command and control systems.

In the cyber domain, attributing the origin of a cyber-attack or distinguishing cyber-attacks from cyber vandalism continue to be complicated topics. However, a peace operation will not face any such issues. Irrespective of the origin of the cyber-attack, the peace operation will continue to respond through self-defense or defense of the mandate. In this regard, the UN needs to play an important role in establishing an institution or mechanism to identify the perpetrators behind cyber-attacks. Various proposals like Digital Geneva Convention or an internationally recognized international cyber court have been proposed in recent times. However, if UNSC mandates a peace operation to maintain law and order, then peacekeepers can resort to employment of all available means for the implementation of the mandate (Kleffner & Dinniss, 2013; Nabeel, 2019).

Scenario C: Offensive Cyber Operations Targeting Civilians in UN Peace Operation's area of Responsibility

If civilians are threatened by cyber operations, then peacekeepers are mandated to resort to use of force for protection of civilians from the imminent threat of physical danger.

[4] The Just War Theory consists of (parameters): Just cause (Defense of self or others against cyberattack); Legitimate authority (The UNSC); Right intent (Defense and justice); Proportionality (Responsive action in proportion to the threat or the magnitude of the original attack); Net benefit (The positive repercussions outweigh the negative ones); Right Conduct (According to a well codified set of "cyber rules of engagement").

However, in case where the imminent threat cannot be established, then it is important to know that the interpretation and operationalization of the term 'imminence' is largely

dependent on the collective consensus of the political leaders, UN departments, the UN force commander and national contingent commanders.

However, it is important to understand that use of force is not the only available option to deal with cyber threats. The threats emanating from cyber domain can be dealt with through technological means such as diverting a Distributed Denial of Service (DDOS) attack stream or blocking a port. Similarly, the mandate to protect civilians is expressed in terms of 'to the extent possible' and 'within mission capabilities'. The UN-approved peace operations possess limited technological capacity for intelligence and information analysis and may not be technologically capable of preventing cyber operations from impacting the civilians. As a mediating party, cyber peacekeepers can utilize mechanism of persuasion or coercion to bring adversaries to the negotiating table.

Additionally, cyber peacekeepers can marshal support from international community and cyberspace stakeholders as a mediating mean (Akatyev & James, 2015). However, if the engagement between peace operation and a State or organized crime reaches such a level of hostility which equalizes the level of conflict, then law of armed conflict is applicable in such a scenario. In this scenario, the right to respond to cyber operation will not remain restricted to self-defense. Peacekeepers will be allowed to lawfully target members of adversary force and their equipment. Likewise, military personnel and the equipment of the peace operation will become lawful targets for other parties of the armed conflict (e.g., Kleffner & Dinniss, 2013).

Scenario D: Peacekeepers Employing Offensive Cyber Operations against Adversaries

As discussed earlier, no publically known cyber operation has ever been conducted against UN peace operation. Similarly, no public cyber operation has ever been conducted by a peace operation (Council on Foreign Relations, n.d.). The 2012 American claim of using cyber operations successfully in Afghanistan cannot be established to be conducted under the auspices of the UN-mandated, NATO-led International Security Assistance Force because of the dual nature of American presence in a war-torn country (Satter, 2012).

For a peace operation likely to be involved in transition phase of reconstruction and development efforts, the ability to turn off a network rather than destroying one might prove to be a more useful tool. Offensive cyber operations will prove advantageous to the UN mission for a number of reasons. Firstly, it may also allow UN peace mission to project its mandate in regions which are beyond its area of deployment and otherwise lacks capabilities to reach those regions. Secondly, cyber operations can be utilized for intelligence and monitoring activities. Thirdly, offensive operations provide peacekeepers with the ability to remotely shut down the networks of opposing actors. This will prove significant in paving a way to disrupt the activities of those who threaten the peace process. Fourthly, offensive cyber operations can also be used as a coercive method in influencing actors involved in peace process.

Fifthly, offensive cyber operations can be undertaken to either remove or blocking online content which incites to commit crimes such as genocide or certain other forms of hate speech. This can only be done if the mandate authorizes any such action. Sixthly, neutralization of command and control networks and air defense

networks might prove as a valuable tool for peace operations. However, the legality of neutralizing (not destroying) a network depends on the categorization of the acts and the operation's mandate. The notion whether mere neutralization of a network by cyber means would amount to an attack under the laws of armed conflict has been subject to extensive debate. According to Tallinn Manual, targeting of networks would be considered an attack only if destruction of the functionality of objects, to include network components, results in physical replacement of a component (Tallinn Manual 105–110). However, the Manual failed to gain wider support and/or recognition (Kleffner & Dinniss, 2013; Nabeel, 2019).

In order to neutralize computers operating outside the area of operations, assistance can be requested from other member states to ensure that their nationals, individuals and firms within their territories refrain from particular offensive behaviors and punish those who engage in such activities. In addition, the peace operation with the support of Internet Service Providers or webhosts, who are based in the geographical area of the peace operation, could either block or redirect the DDoS traffic emanating from particular Internet Protocol (IP) addresses.

Lastly, offensive cyber operations are to be used for non-self-defense circumstances only if authorized by the operation's mandate. In the fulfillment of mission objectives, offensive cyber operations are authorized to cause damage, destruction or physical harm in the same fashion as the kinetic force would be able to do. Similarly, when peacekeepers find themselves involved in hostile engagements under the laws of armed conflict, offensive cyber operations can be deployed in the pursuit of the military objectives (Kleffner & Dinniss, 2013).

Prospects of Establishing UN Cyber-peacekeeping Force

The UN is already deliberating on the term 'digital peacekeeper' which can be defined as a physical peacekeeper (military, police, or civilian), who is equipped with advanced digital equipment to view physical space in conflict zones. Realizing the threats emanating from cyberspace such as cyber-attacks and cyber espionage, the UN is now slowly developing the necessary cyber infrastructure and procedures to protect sensitive information (mission-related information and information about peace operation's adversaries) by preventing break-ins.

The establishment of "Digital Blue Helmets (DBH)" (analogous to physical UN peacekeepers wearing blue helmets) is viewed by experts as an indicative factor showing that UN sees for itself a future role in cyber peacekeeping (e.g., Dorn, 2017). DBH programme proposed a three-tier cybersecurity monitoring mechanism with main 'Global Cybersecurity Monitoring Centre' located in New York. In addition to main monitoring center, there will be regional and non-regional monitoring centers (United Nations Office of Information and Communications Technology, n.d.).

Meanwhile, the UN is exploring its potential role in preventing terrorism in cyberspace. In this regard, the 'UN Counter Terrorism Centre' has plans to help requesting member states to be better capable for preventing terrorist cyber-attacks and mitigating the effects and expediting recovery following the attacks (Dorn, 2017). The UNDPKO is already a part of the associated UN's 'Counter Terrorism Implementation Task Force', which was established in 2005.

In 2013, Chief Executives Board for Coordination adopted seven principles for dealing with cybercrime and cyber security. The seven cyber pillars reflect a UN-system-wide effort to encourage UN programs in helping member states in addressing their cybercrime and cybersecurity needs and take evidence-based action (United

Nations System, 2014).[5] However, all UN efforts in dealing with cyberterrorism and cyber-warfare are in preliminary stages. Experts believe that UN will not be undertaking new roles in regulating activities of states in cyberspace until and unless asked by member states (as cited in Dorn, 2017).

General Framework for Operationalizing Cyber-Peacekeeping Force

The existing literature on cyber peacekeeping has touched upon various aspects of how cyber peacekeepers can undertake the tasks discussed earlier such as creation of cyber buffer zone and implementing observation, monitoring and reporting mechanism. In continuation to the existing knowledge, a brief general framework is presented in this section regarding the operationalization of a future cyber peacekeeping force.

Formulation of Working Modus Operandi

The UN can arrange various sessions (or constitute a GGE) in which government officials, tech companies, non-profit organizations, academia, etc., are informed regarding the requirements of such force. These sessions will serve as the ground work for peacekeeping force which ultimate lead to the materialization of a fully capable force. Some major questions which the UN can put forward during the sessions are;

- What should be the total strength needed for peacekeeping force?
- How future cyber-peacekeepers should be inducted?
- How civilian peacekeepers can join the peacekeeping force?
- How countries will contribute to the force other than personnel? What type of expertise and capabilities will shared by each member state?
- How cyber-peacekeeping force will be funded?
- How to ensure better gender representation in the force?
- How to prevent sexual violence related incidents within the force?
- What guidelines should be formulated to regulate behavior of cyber-peacekeepers?
- What mechanism should be in place to ensure that cyber-peacekeeping force does not become a victim of insider attacks?
- How to bring the good working relationship of physical peacekeepers into cyber peacekeepers?
- What framework should be adopted to investigate cyber-attacks and preventing leakage of sensitive information?

[5] The seven cyber pillars: (1) Cyber incidents should be dealt with in a holistic manner through criminal justice and international cooperation, (2) UN entities should aim to respond to cybercrime and cybersecurity needs in member states within their respective mandates, (3) All UN programming should respect the principles of the rule of law and human rights. (4) UN programming should focus on assisting member states to take evidence-based action, (5) Programming should foster a "whole-of-government" response, (6) Support to member states should aim to strengthen international cooperation, (7) Programming should include efforts to strengthen cooperation between government institutions and private sector enterprises

- How transparency should be maintained in the working modus operandi of peacekeeping force?

Building the Cyber-peacekeeping Force

There are at least four main sources which can contribute cyber-experts for the cyber-peacekeeping force;

(i) ***Troop Contributing Countries***:
A major chunk of cyber-experts will be drawn from UN member states. Unlike physical UN peacekeeping force strength, the major portion of cyber-experts will be drawn from developed countries which have enhanced their cyber capabilities in recent years and have qualified cyber-experts to offer. These cyber-experts will be from both military and police of contributing countries;

(ii) ***Cyber Contributing Organizations:***
Organizations like tech companies can offer their cyber-experts on periodic basic to the force;

(iii) ***Volunteers:***
A significant portion of cyber-experts can be drawn as civilian peacekeepers who volunteers their time for the force. These peacekeepers can range from independent cyber-experts to academicians.

(iv) ***UN Cyber Staff:***
For the smooth operational working of cyber peacekeeping force, it is important to have a dedicated full time UN staff. These officials will mainly be responsible for administration and coordination related tasks (Robinson et al., 2018).

Locating Cyber-Peacekeeping Force and Virtual Collaborative Environment (VCE)

The cyber-peacekeeping force can easily be embedded in the current hierarchical structure of UN peacekeeping. Instead of segregating cyber-experts into military, police and civilian peacekeepers, it is ideal to combine all those experts into a dedicated and distinct cyber unit. With regards, defined as digital spaces where remotely located people can come together and interact with each other and with virtual objects, Robinson and colleagues (2018) proposed adoption of such mechanism for cyber-peacekeeping force with four pre-requisite. They suggest that the VCE should be able to; cater to both small and large scale cyber peacekeeping activities; reliable in the sense that it can accept concurrent users with no failures of availability; secure since it will be containing sensitive information; and, contain resource sharing component, Voice over Internet Protocol and reporting system.

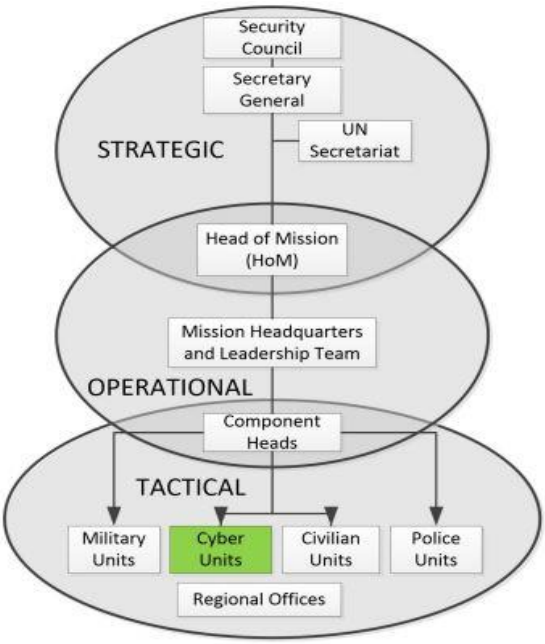

Figure 1: Proposed UN Peacekeeping Organizational Structure (Robinson, Jones, Janicke & Maglaras, 2018)

Conclusion

In years to come, cyber operations are likely to be directed at UN peace operations or used by peace-keeping operations in the implementation of their mandates. However, creation of full fledge UN cyber-peacekeeping force seems a far-sighted idea at this point in time. What is more likely to occur in the near future is addition of unit comprising cyber-experts from troop contributing countries, tech companies, non-profit organization, volunteers to UN peace operations, which will be utilized for both offensive and defensive cyber operations.

Prior to formulation of such a dedicated unit or force, it is important to address all the underlying legal hurdles regarding the conduct of such a unit or force. Similarly, the jurisdiction of this unit or force should be clearly mentioned in the peace operation's mandate as authorized by UNSC so as to not leave any form of ambiguity. On the other hand, it is important for organizations involved in peacekeeping efforts to create awareness about cyber threats and assist other organizations in undertaking measures to secure themselves from cyber-attacks.

While debating about the feasibility of a cyber-peacekeeping force continues, it is important for all major stakeholders; governments, non-profit organizations, tech companies and academia – to create awareness among the users about the threats emanating from cyberspace. This awareness campaign and subsequent citizen actions can alone contribute in resolving about 80 per cent of daily cybersecurity threats (e.g., Sanger, 2018). Apart from awareness initiatives, efforts should also be undertaken by major stakeholders for formulating legal frameworks based on punishing cybercriminals and similar offenders and ensuring measures for cybersecurity i.e. defending critical infrastructure and key commercial enterprises.

References

Akatyev, N., & James, J. I. (2015, October). Cyber peacekeeping. In *International Conference on Digital Forensics and Cyber Crime* (pp. 126-139). Springer. Retrieved from https://www.researchgate.net/profile/Joshua_I_James/publication/300144087CyberPeacekeeping/links/5721741608ae82260fab44b6/Cyber-Peacekeeping.pdf.

Cahill, T. P., Rozinov, K. & Mule, C. (2003). Cyber Warfare Peacekeeping. *Proceedings of the 2003 IEEE Workshop on Information Assurance*. Retrieved from https://ieeexplore.ieee.org/document/1232407.

Council on Foreign Relations (n.d.). Cyber Operations Tracker. *Council on Foreign Relations*. Retrieved from https://www.cfr.org/interactive/cyber-operations.

Dorn, W. (2017). Cyberpeacekeeping: A New Role for the United Nations. *Georgetown Journal of International Affairs* 18, 138.

Dorn, A. W., & Webb, S. (2019). Cyberpeacekeeping: New Ways to Prevent and Manage Cyberattacks. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *9*(1), 19-30.

Grisby, A. (2018, November 15). The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased. *Council on Foreign Relations*. Retrieved from https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

International Covenant on Civil and Political Rights. (1966). *International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI), U.N. Doc. A/6316* (Dec. 16, 1966), 999 U.N.T.S. 171.

Kleffner, J. K. and Dinniss, H. A. H., (2013). Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations. *International Law Studies*, *89*, 512-535. Retrieved from https://digital-commons.usnwc.edu/ils/vol89/iss1/4/.

Markoff, J. (2008, August 12). Before the Gunfire, Cyberattacks. *New York Times*. Retrieved from https://www.nytimes.com/2008/08/13/technology/13cyber.html.

Nabeel, F. (2019). International Cyber Regime: A Comparative Analysis of the US-China-Russia Approaches. *Stratagem*, *1*(2), 8-27. Retrieved from https://journal.cscr.pk/stratagem/index.php/stratagem/article/view/22.

Phneah, E. (2012, February 6). Idea of Cyber Peacekeepers Premature, 'Redundant'. *ZDNet.* Retrieved from https://www.zdnet.com/article/idea-of-cyber-peacekeepers-premature-redundant/.

Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2018). An Introduction to Cyber Peacekeeping. *Journal of Network and Computer Applications*, *114*, 70-87.

Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2019). Developing Cyber Peacekeeping: Observation, Monitoring and Reporting. *Government Information Quarterly*, *36*(2), 276-293.

Sanger, D. E. (2018). *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. USA: Crown Publishing Group.

Satter, R. (2012, August 24). US General Says His Forces Carried Out Cyberattacks on Opponents in Afghanistan. *Associated Press*. Retrieved from http://seattletimes.com/html/nationworld/2018983462_apusafghancyberattacks.html.

Tallinn Manual, supra note 24, at 105–110.

United Nations Charter Article 39.
United Nations Charter Article 41.
United Nations (2013). 68/167. The Right to Privacy in the Digital Age. United Nations General Assembly 68th Session. Retrieved from https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167
United Nations Office of Counter-Terrorism. (n.d.). Coordination and Coherence of the Counter-terrorism Efforts of the United Nations. *United Nations Office of Counter-Terrorism*. Retrieved from https://www.un.org/counterterrorism/ctitf/en/structure.
United Nations Office of Information and Communications Technology. (n.d.). Digital Blue Helmets. *United Nations Office of Information and Communications Technology*. Retrieved from https://unite.un.org/digitalbluehelmets/sites/unite.un.org.digitalbluehelmets/files/docs/digitalbluehelmets_brochure_final.pdf.

United Nations System. (2014, January 13). Chief Executives Board for Coordination, Summary of Conclusions, Second Regular Session of 2013. *United Nations System.* Retrieved from https://www.unsceb.org/CEB PublicFiles/Chief%20Executives%20Board % 20for% 20Coordination/Document/REP _CEB_201311_CEB2013-2.pdf