DEFENCE AND DIPLOMACY

IN PURSUIT OF NATIONAL SECURITY

VOL. 12 NO. 1 ISSN 2347 - 3703 OCTOBER-DECEMBER 2022

JOURNAL OF THE CENTRE FOR AIR POWER STUDIES

CYBER PEACEKEEPING: PROSPECTS FOR INDIA

DIVYANSHU JINDAL

INTRODUCTION

In August 2021, India held the presidency of the United Nations Security Council and presided over the ministerial-level open debate on 'Technology and Peacekeeping'.[1] India's presidential statement called for recognising that 'technology has the potential to act as a force multiplier', and India's External Affairs Minister (EAM), S. Jaishankar—remarked that to adapt to increasingly complex global dynamics, UN Peacekeeping Operations (UNPKOs) "must be anchored in a strong ecosystem of technology and innovation".[2] India proposed a four-point framework laying down architecture for securing UN peacekeepers from contemporary

Mr **Divyanshu Jindal** is Research Associate at the Centre for Air Power Studies, New Delhi.

[1] Geeta Mohan, "India's Three-Point Agenda at UN Security Council", *India Today*, August 3, 2021, at https://www.indiatoday.in/india/story/india-un-security-council-august-presidency-agenda-maritime-security-counterterrorism-peacekeeping-1836364-2021-08-03. Accessed on August 3, 2022.

[2] "Peacekeeping Must Be Anchored in Strong Ecosystem of Technology, Innovation", *Hindustan Times*, August 19, 2021, at https://www.hindustantimes.com/india-news/peacekeeping-must-be-anchored-in-strong-ecosystem-of-technology-innovation-eam-at-unsc-debate-101629313721725.html. Accessed on August 5, 2022.

threats.[3] Among these points was the need to focus attention and infuse investment towards consistent training and capacity building of peacekeepers in the field of technology. It was highlighted that while new technologies help peacekeepers in their mandates, it also makes them vulnerable to risks in the cyber domain. UN Secretary-General Antonio Guterres underlined the increasing danger of anonymous actors with the intent and capabilities to attack critical infrastructures which are crucial to societal functioning.[4]

India has proven its commitment to peacekeeping time and again. India has achieved remarkable success in peacekeeping operations in high-risk environments and now seeks to help towards capacity building in the domain of technology. In his statement, EAM Jaishankar highlighted that, "UNPKO cannot afford to cede the information advantage to those actors determined to undermine peace by using modern technology to aid their violent cause".[5] India supports the UN C4ISR (UN Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) Academy for peace operations.[6]

The UN has been developing infrastructure and procedures to safeguard the UNPKOs from risks emerging from the cyber domain. The cyber peacekeeping (CPK) concept is not new; however, not much debate has happened among the "most UNPKO troop-contributing nations" over this topic. The 'Digital Blue Helmets' (DBH) programme, launched by the UN in 2016 under its Office of Information and Communications Technologies (OICT), was a continuation of a series of steps by the UN over the past decade towards incorporating cyberspace within its framework.[7] This has

[3] "Harness Digital Technology to Protect Peacekeepers, Civilians, Security Council Urges, Adopting Presidential Statement", UN Meetings Coverage and Press Releases, August 18, 2021, at https://www.un.org/press/en/2021/sc14607.doc.htm. Accessed on August 3, 2022.

[4] n. 2.

[5] n. 3.

[6] Aarshi Tirkey, "Maritime Security, Peacekeeping, and Counterterrorism: Pillars of India's UNSC Presidency", Observer Research Foundation, October 5, 2021, at https://www.orfonline.org/research/maritime-security-peacekeeping-and-counterterrorism/. Accessed on August 5, 2022.

[7] Fahad Nabeel, "Cyber Peacekeeping: Critical Evaluation of Digital Blue Helmets Program", *NUST Journal of International Peace and Stability*, July 23, 2020, at https://doi.org/10.37540/njips.v3i2.53. Accessed on August 7, 2022.

been viewed as an indicative factor showing how the UN sees its future potential role in CPK.[8]

While India's intent towards contributing to technology sectors is visible, its capability to do so is often questioned. For UN CPK, it will be essential for nations to develop their cyber capabilities before they can seek a leadership role in global peacekeeping efforts in cyberspace. To this aim, it is necessary to increase awareness and pursue discussions revolving around the necessities, challenges, and benefits of CPK. This study aims to provide a brief background on the concept of CPK, recent developments in global geopolitics relevant to CPK, and India's prospects in this direction. While there are several resources which investigate the intricacies of peacekeeping and cyber peacekeeping, this study attempts to take ahead India's intent in technology domains in the UN and connect it with the possibilities of continuing India's leadership in the cyber domain.

CYBER PEACEKEEPING

In its traditional form, peacekeeping involves keeping warring factions away from each other in an internal conflict or civil war, or between two or more nations in case of an international conflict.[9] UN peacekeeping (UNPK) is guided by principles like consent of parties, impartiality, and non-use of force, except when in self-defence or defence of the mandate. As conflicts have become increasingly digitised, with wars now being waged online using misinformation and social media, and on critical infrastructures—like water and energy facilities—through cyberspace, peacekeeping efforts will need to adapt to this changing reality as well.

According to Nikolay Akatyev and Joshua James, CPK can be defined as "cyber conflict prevention, mitigation, aftermath containment, and rehabilitation with a focus on conflict de-escalation

[8] Fahad Nabeel, "Integrating Cyber-Peacekeeping Unit within the UN Peacekeeping Force", Centre for Strategic and Contemporary Research, September 29, 2019, at https://cscr.pk/explore/themes/defense-security/integrating-cyber-peacekeeping-unit-within-the-un-peacekeeping-force/. Accessed on August 5, 2022.

[9] Syed Hasnain, "UN Peacekeeping Operations: Why India's Peacekeepers Are Sought After", IBN Live, September 28, 2015, at https://indianarmy.nic.in/writereaddata/documents/article290915.pdf. Accessed on August 7, 2022.

and civilian security".[10] In their view, the main goal is to promote online safety and security through international laws and agreements. Another definition defines CPK as "cyber-related action undertaken to preserve peace, however fragile, where fighting has halted and to assist implementing agreement achieved by peacekeepers".[11]

It is expected that future conflicts will invariably have a cyber component. Various scenarios can deem it necessary for UN PKOs to deploy cyber units. Some of the possible scenarios as highlighted by Fahad Nabeel can be:[12]

- Peacekeepers deployed in a region marred by offensive cyber operations
- Offensive cyber operations targeting UN operations
- Offensive cyber operations targeting civilians in UN peace operation's area of responsibility
- Peacekeepers employing offensive cyber operations against adversaries.

If the UN Security Council (UNSC) determines that cyberwarfare could amount to a threat to international peace and security, it can permit cyber peacekeeping and use the International Human Rights Law (IHRL) to guide the framework of the mandate of the UN CPKO. For this, Article 39 of the UN Charter can be utilised.[13] However, the UN can also use Article 41 of the UN Charter if the threshold for armed conflict is crossed, thereby making the law of armed conflict applicable to CPKOs as well.[14]

Several ways have been suggested by academia and think tanks to assimilate CPK into the current hierarchical structure of UNPK. These involve establishing a distinct cyber unit comprising cyber experts, who either volunteer, are offered by tech companies, contributed by troop-contributing nations, or are dedicated full-time

[10] Nikolay Akatyev and Joshua James, "Legislative Requirements for Cyber Peacekeeping", *The Journal of Digital Forensics, Security and Law* 12, no. 3 (2017), at https://doi.org/10.15394/jdfsl.2017.1447.\\uc0\\u8221. Accessed on August 4, 2022.

[11] Michael Robinson et al., "An Introduction to Cyber Peacekeeping", *arXiv*, April 24, 2018, at http://arxiv.org/abs/1710.09616. Accessed on August 4, 2022.

[12] n. 8.

[13] Robinson et al., n. 11.

[14] n. 8.

to UN CPKOs.[15] In recent years, there have been steps taken towards this goal. With necessity rising, the possible roles and the challenges have been articulated.

Necessity

It is now increasingly argued that cyberwarfare is upon us. With conventional wars now involving cyber as a strategic domain, in recent years, a large proportion of research has focused on understanding how cyberwarfare would be conducted. As war transforms into a 'hybrid war', consequences for societal well-being are becoming unpredictable by the day. In the past decade, election interferences, hacks into critical infrastructure, and ransomware attacks broke records. This has resulted in nations vying to achieve cyber capabilities, both defensive and offensive. As defending cyberspace becomes a priority towards safeguarding national sovereignty and rights for the citizenry, a security dilemma resulting from the increasing militarisation of cyberspace is being debated today.

Also, compared to traditional forms of militarisation attempts, cyberspace is much more complex. Cyberweapons can easily proliferate through replication and encryption, without much cost or logistics. Another key factor in restricting the militarisation of cyberspace emerges from the fact that the same asset—code, programme, or software—can be used for cyber defence and cyber offence. Thus introducing ambiguity.

It is argued that if cyberattacks could lead to state collapse due to failure of critical national infrastructure—resulting in humanitarian suffering and human rights abuses and threats to international peace and security—CPKs will become necessary for safeguarding the services essential for running a nation (e.g., water supplies, banking, power grids, transportation). Inaccessibility to information due to destruction of internet infrastructure or blocking of service through cyberattacks like the Distributed-Denial-of-Service (DDoS) attacks, can further necessitate CPK efforts. In fragile and conflict-prone nations, electoral integrity can be harmed through the cyber

[15] Fahad Nabeel, "Establishment of UN Cyber Peacekeeping Force: Prospects and Challenges", *NUST Journal of International Peace and Stability*, July 25, 2019, at https://doi.org/10.37540/njips.v2i2.29. Accessed on August 9, 2022.

domain in several ways like manipulation of voters through social media, or direct election result tampering. All these scenarios present a situation which can escalate to retaliatory actions by a victim. As accurate attribution in the cyber domain remains a complex issue, this can result in an unintended and wrongly-directed disaster.

The UN Secretary-General Strategy for the Digital Transformation of UN Peacekeeping 2021 highlighted that cyberattacks for financial gain, destruction or disruption of critical infrastructure, Intellectual Property (IP) theft or commercial espionage, have been on the rise and have begun to target CPK.[16] However, while cyber technologies can be used to impede the implementation of UNPK mandates, they can also be used for assisting peacekeepers to address challenges. The 2015 UNM Report of the High-Level Panel on Peace Operations stressed the need for implementing new technologies in UNPKOs as a way to promote international security and stability.[17] This includes the cyber domain.

It has to be noted that UNCPK, like the traditional UNPK, is not explicitly stated in the UN Charter. But, under the doctrine of implied powers, the UN is "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".[18] Thus, UN CPKO can be based on Articles 10, 11, 12 and 22 of the UN Charter, which mention the broad powers of the UN on international peace and security matters. However, the UN will derive its power to act from its members and will remain dependent on them for resources and manpower too. For any nation to chalk out its stance towards CPK, it is important to understand the possible roles that UN CPK is expected to take on and the available alternatives.

[16] "Strategy for the Digital Transformation of UN Peacekeeping", United Nations Peacekeeping, at https://peacekeeping.un.org/en/strategy-digital-transformation-of-un-peacekeeping. Accessed on August 7, 2022.

[17] Nicholas Tsagourias and Giacomo Biggio, "Cyber Peacekeeping Operations and the Regulation of the Use of Lethal Force", *International Law Studies* 99, no. 1 (February 4, 2022), at https://digital-commons.usnwc.edu/ils/vol99/iss1/3. Accessed on August 6, 2022.

[18] Ibid.

Possible Roles and Recent Developments

As observed in the scenarios above, numerous possibilities for misunderstandings and misattributions due to the opaque and complex character of cyberspace, create opportunities for CPK. Several studies have highlighted these wide-ranging opportunities which cover areas lie support to member states for capacity building to manage cyber ceasefires. Some of the areas where cyber peacekeepers can be deployed are:[19]

- Monitoring actions in cyberspace that may violate peace agreements between conflicting parties (a form of the cyber ceasefire).
- Creation and maintenance of a cyber buffer zone towards the objective above.
- Monitoring human rights abuses in mandated cyberspace.
- Disarmament of cyberweapons.
- Demobilisation of cyber combatants (by re-purposing their cyber skills towards noble objectives).
- Managing warning system for impending cyberattacks and ongoing operations.
- Working towards the attribution problem by supporting nations lacking cyber attribution capacities.
- Electoral assistance to maintain democratic integrity.
- Actively conducting the 'mine actions' which would involve scanning, documenting, isolating, and cleaning infected systems, malware, and cyber threat education, and supporting the development of national malware action capacity.

Beyond the above tasks, CPK efforts can be directed towards broader mandates of observation or monitoring. CPK can be utilised to monitor violations of freedom of expression and access to information which is deemed valuable towards maintaining peace. It can also monitor any emerging and potential flashpoints of cyber conflict, and patterns of botnet formation and network structure changes. Many mechanisms have emerged towards these goals in recent years, both in the UN and outside.

[19] Nabeel, n. 8 and Robinson, et al., n. 11.

The DBH programme[20] (as defined earlier) had proposed a three-tier cybersecurity monitoring mechanism. With a main 'Global Cybersecurity Monitoring Centre' located in New York, the US, additional regional and non-regional monitoring centres were envisioned. The programme is seen as an effort to build capacity, strengthen coordination, and foster collaboration against information technology security incidents for the UN. The DBH remains an internal cybersecurity team for the UN and does not currently have an expansive mandate.

While the UN Volunteers (UNV) programme, which annually deploys volunteers professionals with UN PKOs, can be a model extended to the cyber domain and a 'Cyber Peace Corps' can be established, initiatives from the private sector and non-governmental sector have also emerged. One such example is the 'CyberPeace Builders' programme coordinated by the Switzerland-based CyberPeace Institute.[21] The programme aims to assist Non-Governmental Organisations (NGOs) in building cybersecurity capacity through a trusted and dedicated network of corporate partners who provide volunteers and funding to enable the provision of this support.

However, for CPK effort to reach a point of consensus and gain a mandate in conflicts in future, it is argued that it will have to overcome challenges like 'political resistance at all levels', technical hurdles, and manpower bottlenecks.

Challenges

Challenges to CPK are multifold. First, there exist technical challenges associated with the capabilities and infrastructure required for high-level CPK efforts. As nations use complex cyber defence mechanisms and attackers are becoming more sophisticated in their strategies and skills by the day, CPK efforts will need to match these as well. Beyond this, manning the cyber units for peacekeeping purposes will be an uphill task, especially considering that most nations are now

[20] "UN Digital Blue Helmets", at https://unite.un.org/digitalbluehelmets/. Accessed on August 2, 2022.

[21] "CyberPeace Builders", CyberPeace Institute, October 13, 2021, at https://cyberpeaceinstitute.org/cyberpeacebuilders/. Accessed on August 5, 2022.

trying to satisfy their own manpower needs having cyber expertise, and the shortage in this sphere remains an issue of concern. The mechanisms for cyber troop contributions have still not been a part of discussions over CPK. The role of private organisations, NGOs, and governmental bodies in CPK needs much deliberation.

Like most global efforts and multilateral platforms, CPK will also have to wrestle with funding issues. As attribution technologies are still in nascent phases, that too only among a handful of member states, the costs for achieving CPK capabilities and then conducting operations, might be a more costly prospect than the UN, and even most member states, can afford to pursue. Further, without a proper legal framework or universally agreed cyber policy or law, CPK will face resistance at local, regional, and national levels.

THE WAY AHEAD FOR INDIA

India has a long and distinguished history of service in UN peacekeeping. The South Asian nation has contributed more personnel than any other country, with more than 244,500 Indians who have served in 49 of the 71 UNPK missions since 1948.[22] India enjoys strong goodwill and support at the UN and has been elected to several UN bodies. While Indian efforts are incomparable and remarkable in every aspect, a parallel can be drawn with Canadian efforts in terms of importance given to peacekeeping throughout the history of the concept.

For Canadian foreign policy, peacekeeping has been a central theme for over 60 years when Lester Pearson played a leading role in developing the concept in response to the Suez Crisis.[23] Even though the Canadian efforts have dwindled since the 1990s, recent years have witnessed efforts in renewing Canada's commitment to peacekeeping. Canada adopted a defence policy—*Strong Secure Engaged* (SSE)—which committed billions of dollars to cyberinfrastructure and

[22] "India and the United Nations", Ministry of External Affairs India, at https://mea.gov.in/Portal/ForeignRelation/India_UN_2020.pdf. Accessed on August 1, 2022.

[23] "Peacekeeping? It's an Age Thing", Canadian Global Affairs Institute, November 2020, at https://www.cgai.ca/peacekeeping_its_an_age_thing. Accessed on August 8, 2022.

programming.[24] Since 2015, Canada has contributed over US$ 13 billion to cyber capacity-building projects around the world and supported the development or improvement of 17 CERTs in the Americas.[25] Canada has also engaged in implementing Confidence Building Measures (CBMs) internationally, in the cyber domain. In recent years, Canada has sought to develop cyber attribution capabilities and policies and has engaged in public attribution of malicious cyber activities to the hostile states, separately and in joint effort with partners like the US and the EU.[26] Canada has established its armed forces for a cyber domain which includes both reserve and regular members who conduct cyber defence operations. A 2019 report by the Canadian Association of Defence and Security Industries (CADSI) highlights that the Canadian industry leads in cyber defence capabilities in many areas, and the Canadian government has attained expertise in cyber oversight, threat intelligence, investigation, reactive cyber and quantum cryptography through significant investments in the cyber domain.[27] As Canada aims to make a comeback in leadership roles on global issues, especially in the UN, CPK is seen by many experts as a way to harness Canada's governmental apparatus and industrial potential.

A similar case needs to be made for India. It is argued that New Delhi has demonstrated time and again that it is not merely a large troop contributor to UNPK missions but is equally capable of introducing new initiatives and ideas.[28] Justifying its potential, India needs to seek to shape the important global agendas that are going to affect international peace and security in the coming years and take a leadership role in establishing capabilities. Undoubtedly, the cyber

[24] "From Bullets to Bytes: Industry's Role in Preparing Canada for the Future of Cyber Defence", Canadian Association of Defence and Security Industries, 2019, at https://www.defenceandsecurity.ca/UserFiles/Uploads/publications/reports/files/document-24.pdf. Accessed on August 10, 2022.

[25] "International Cyber Policy", Government of Canada, April 22, 2022, at https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyber_policy-politique_cyberspace.aspx?lang=eng. Accessed on August 14, 2022.

[26] Ibid.

[27] n. 24.

[28] n. 6.

domain and CPK is a ripe avenue for realising India's ambitions for a better position on the global political high table.

It can be argued that several other contenders, with impressive cyber expertise and capabilities—in technology, funding, and manpower—may be either not interested in CPK (being disinterested in the prospect of sharing technology) or might not be supported by other nations (due to lack of trust). This can be exemplified by taking the context of current geopolitical dynamics where the world is divided between the eastern and the western blocs, with China and Russia being increasingly countered by the US and the EU in every realm, be it economic, defence or technology, much like the Cold War era. In this light, India has the chance to again provide an alternative and provide a third way for international security and peace.

India's efforts towards establishing its cyber capabilities in recent years have been noted and appreciated. India was placed 10th in the Global Cyber Security Index 2020 which measures the commitment of countries to cybersecurity at a global level.[29] Further, India's cybersecurity industry has reportedly nearly doubled in size between 2019 and 2021, with the workforce increasing from 110,000 to 218,000 and revenues from cybersecurity products and services growing from around US$ 5 billion to US$ 9.85 billion.[30] India's cybersecurity start-up and product industry have also witnessed robust growth. In cybersecurity, India can leverage its industrial potential where service-based companies can leverage their global expertise and experience in offering 'transformational and platform-based services'.[31] So, just like Canada, India has the benefit to utilise its domestic cybersecurity potential, in the global arena.

[29] Sandhya Sharma, "India Breaks into Top 10 Countries on UN's Index Measuring Commitment to Cybersecurity", *The Economic Times*, June 29, 2021, at https://economictimes.indiatimes.com/news/defence/india-breaks-into-top-10-countries-on-uns-index-measuring-commitment-to-cybersecurity/articleshow/83962167.cms?from=mdr. Accessed on August 10, 2022.

[30] Aron Tan, "India's Cyber Security Industry Doubles in Size amid Pandemic", ComputerWeekly.com, January 24, 2022, at https://www.computerweekly.com/news/252512351/Indias-cyber-security-doubles-in-size-amid-pandemic. Accessed on August 10, 2022.

[31] Ibid.

CONCLUSION

Cyber conflicts will rise as the cyber domain becomes increasingly integrated into defence frameworks and strategic considerations. With digital/virtual reality now a part of the societal psyche, the cyber domain will pose vulnerabilities to national and international security, and therefore, CPK efforts will be an unavoidable aspect of efforts at maintaining peace at domestic and global levels. While the concept of UN CPK is not new, its development of this concept has remained slow. With multiple challenges ranging from the technical nature of cyberspace to financial bottlenecks, 'political will' would be a key aspect for progress in attaining peace in cyberspace. India has been a reliable and proud peacekeeper under the aegis of the UN. As the world transforms at an accelerated pace, posing new challenges, it is another opportunity for India to realise its potential on the global podium.