Cyber Peacekeeping: Critical Evaluation of Digital Blue Helmets Program

NUST Journal of International Peace & Stability
2020, Vol. III (2) Pages 17-27
njips.nust.edu.pk

Fahad Nabeel[1]

Abstract
In 2016, the United Nations (UN) launched the Digital Blue Helmets (DBH) program under its Office of Information and Communications Technologies (OICT). The launching of DBH was a continuation of a series of steps that the UN and its related agencies and departments have undertaken over the past decade to incorporate cyberspace within their working methodologies. At the time of inception, DBH was envisioned as a team capacitated to act as a replica of a physical peacekeeping force but for the sole purpose of overseeing cyberspace(s). Several research studies have been published in the past few years, which have conceptualized cyber peacekeeping in various ways. Some scholars have mentioned DBH as a starting point of cyber peacekeeping while some have proposed models for integration of cyber peacekeeping within the current UN peacekeeping architecture. However, no significant study has attempted to look at how DBH has evolved since its inception. This research article aims to examine the progress of DBH since its formation. It argues that despite four years since its formation, DBH is still far away from materializing its declared objectives. The article also discusses the future potential roles of DBH, including its collaboration with UN Global Pulse for cyber threat detection and prevention, and embedding the team along with physical peacekeepers.

Keywords
Cyber peacekeeping, Cyberspace, Digital Blue Helmets (DBH), peacekeeping

Introduction
Since 1948, United Nations peacekeeping missions have undergone gradual transformation (Akatyev & James, 2017). From the initial deployments for solely dealing with inter-state conflicts, the structure of peacekeeping missions transformed in the late 1980s to incorporate deployment for intra-state conflicts and civil wars (Kenkel, 2013; Solà-Martín & Woodhouse, 2011). Over the decades, peacekeeping missions followed the traditional model of military deployment for various political purposes like monitoring ceasefires and patrolling buffer zones between hostile parties. However, a growing number of UN operations are becoming multidimensional with the involvement of multiple stakeholders and wide-ranging mandates (United Nations, 2003). The current thirteen UN peacekeeping missions have diverse nature of mandates from observing ceasefire line in disputed Jammu and

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

Kashmir to protecting civilians and consolidating peace in the Democratic Republic of Congo (United Nations Peacekeeping, n.d.).

While technological advancements have transformed the global political and economic landscape, the same technologies are also being used to disrupt the political, economic and social orders in various parts of the world. The disruption is occurring in the form of cyber-attacks, cyber-enabled disinformation campaigns and other strands of cybercrimes. However, the UN peacekeeping operations currently do not deal with challenges emanating from cyberspace and lack functionality with respect to the launch of cyberspace operations (Akatyev & James, 2017). This is primarily so because the traditional UN peacekeeping operations are not authorized to employ potential cyber peacekeepers in the following four situations which generally lead towards peacekeeping mandate (United Nations Peacekeeping, n.d.);

- Preventing or limiting the spread of conflicts;
- Facilitating the implementation of peace agreements;
- Stabilizing conflict regions after a ceasefire is reached;
- Assisting post-conflict states in their transition to a stable government.

Therefore, the UN makes itself incapable of incorporating cyber component in peacekeeping missions (Almutawa, 2020). Additionally, the UN is handicapped in terms of knowledge and human resources in dealing with cyberspace related threats (Dorn, 2017). The international organization also lacks in-depth knowledge about threats emanating from cyberspace and cyberwarfare capabilities possessed by various countries. The rapid advancement in information and communications technology demands further transformation in UN peacekeeping (Nabeel, 2019). In this regard, the United Nations launched the DBH program in 2016. It was one of the several measures taken by the organization in the past few years for promoting cyber safety worldwide (Office of Information and Communications Technology, n.d.).

The DBH unit was created under the UN's Office of Information and Communications Technologies (OICT). It was formed to "enhance cybersecurity preparedness, resilience and response" to protect the UN and its agencies. By incorporating the term *Blue Helmets*, there is a possibility that the unit can prevent, mitigate and deal with future global cyberattacks (Dorn & Webb, 2019, p. 22).

Before DBH's launch, some research studies re-centred their focus to conceptualize cyber peacekeeping (Akatyev & James, 2015; Cahill et al., 2003; Kleffner & Dinniss, 2013). Some scholars viewed DBH as starting point for cyber peacekeeping (Akatyev & James, 2017) while others were proposing various models for integrating cyber peacekeeping within current UN peacekeeping architecture (Robinson et al., 2019; Almutawa, 2020). However, no significant study has so far attempted to explore how DBH has evolved since its formation in 2016. Considering this gap, this research article investigates the objectives behind the formation of DBH and how the programme has evolved to fulfil those objectives.

Despite its formation in 2016, there is still limited data points and limited availability of literature regarding day to day functionality of the DBH program. There are two main reasons for this. Firstly, DBH has to maintain secrecy regarding its internal operations. This practice is in lines with how traditional intelligence agencies operate in terms of their routine functionality. Secondly, the mandate of DBH is not very expansive in nature. Simply put, it is not for cyber peacekeeping. DBH is doing for the UN what any cybersecurity department does within an

organization to secure it from external attacks (Personal communication, June 12, 2020).

To overcome this limitation, this article heavily relies on the publically available information released by UN OICT, interviews given by UN Chief Information Technology Officer (CITO) Atefeh Riazi about the DBH initiative and what former employees have publically shared about their activities at the DBH. Additionally, an interview was also conducted with Professor Walter Dorn of Royal Military College & Canadian Forces College who has been in contact with the DBH team and has been following the initiative since its formation. The analysis of the literature gathered from primary and secondary sources has facilitated the conclusion that DBH is still far away from materializing its proposed objectives.

In the first part of this article, a synopsis of how the UN and its related agencies and departments are incorporating cyberspace within their operations is presented. The second part provides an introductory profile of the DBH program. This is followed by the current progress of DBH in materializing its objectives and how it has evolved ever since its creation. The concluding section of the article aims to understand the potential roles that DBH can play in future and provides recommendations on how an entity can further improve itself in the long run.

Understanding UN Cyberspace-related Activities

Before discussing the DBH programme, it is essential to develop an understanding of the activities undertaken by the UN concerning cyberspace. In this technological era, different agencies and departments within the UN are paying attention to cyberspace in various ways. In 2009, the UN Global Pulse program was initiated to employ big data and Artificial Intelligence (AI) to large-scale data analysis for humanitarian challenges and predict humanitarian catastrophes (UN Global Pulse, 2012; Global Pulse, n.d.).

Since 2011, International Multilateral Partnership against Cyber Threats (IMPACT) — an organization bringing together various stakeholders to enhance the global community's capabilities in dealing with cyber threats — has acted as the cybersecurity executing arm of the International Telecommunication Union (ITU). Due to this role, it has been offering assistance and support to ITU member states and organizations within the UN system in terms of cybersecurity and cybercrime-related issues (Digital Watch, n.d.). However, IMPACT has limited scope due to several factors which include no involvement of major national cyber powers and a focus of the organization on training and monitoring for businesses (Akatyev & James, 2017, p. 5).

In 2016, four UN-related agencies and departments — the International Telecommunication Union, the United Nations Conference on Trade & Development, the United Nations Interregional Crime and Justice Research Institute and the United Nations Office on Drugs & Crime — collaborated with World Bank and other organizations to create 'Combatting Cybercrime: Tools and Capacity Building for Emerging Economies' toolkit. This toolkit aimed to empower policymakers, legislators, public prosecutors & investigators, and civil society of developing countries to enhance their capacity in the policy, legal and criminal justice aspects to combat cybercrime (Combatting Cybercrime, n.d.).

The UN Secretary-General António Guterres convened a High-level Panel on Digital Cooperation in July 2018. The objective behind convening such a panel was to strengthen cooperation in the digital space among various stakeholders ranging

from governments to the technical community (Digital Cooperation, n.d.). Additionally, the prime functions of the Panel are raising awareness about the impact of digital technologies across society and contributing to public discourse pertaining to safe and inclusive digital future for all while taking into account relevant human rights norms.

The Panel submitted a report titled *The Age of Digital Interdependence* to the Secretary-General in June 2019 (United Nations, 2020). The report explained how digital technology could help in achieving Sustainable Development Goals (SDGs) and a more inclusive digital economy. Taking into account issues related to human rights, human agency and security in the digital realm, the report proposed on how to improve digital cooperation architecture (United Nations, n.d.). The report and follow-up discussions have been incorporated in UN Secretary-General's Roadmap on Digital Cooperation. The report states that "digital technologies can support United Nations peacekeeping efforts globally, including by ensuring the safety and security of peacekeepers" (Report of the Secretary-General Roadmap for Digital Cooperation, 2020).

The ITU also maintains the Global Cybersecurity Index. The index is a multi-stakeholder initiative to measure the commitment of countries to the ITU's Global Cybersecurity Agenda. The rationale behind the formation of the index is to forge international cooperation and promote knowledge exchange on this topic (International Telecommunication Union, n.d.). The United Nations Office on Drugs and Crime oversees Global Programme on Cybercrime. The programme has been formed to assist member states in terms of capacity building and technical assistance against cyber-related crimes (United Nations Office on Drugs and Crime, n.d.). Currently, increased usage of technology by peacekeeping operations has been observed. However, the operations are limited in data, tools analysis and human resources for information processing. Similarly, there is no keen interest in incorporating cyberspace into peacekeeping efforts (Akatyev & James, 2017, p. 5).

Introductory Profile about Digital Blue Helmets Program

The DBH team consists of cybersecurity practitioners specializing in cyber audit and assessment, big data, data analysis, event monitoring, digital forensics, operations and environment testing. It currently functions out of the OICT, Department of Management in New York (United Nations Careers, n.d.). UN CITO Atefeh Riazi explained the rationale behind the formation of DBH as potential peacekeepers who "can operate in the cyber world protecting the UN from cyber intrusion, and helping our substantive arms in delivering their missions in the cyber world" (Tucci, 2016).

Recruitment for DBH started around February 2016. Human trafficking was one of the primary issues which the team was to focus upon its formation in addition to playing a decisive role in cybersecurity and combating cybercrime. The ultimate aim of DBH, as explained by Atefeh Riazi, was "a model for creating what we are calling the light web. When we dream about developing a light web to counteract the evil part of the dark web, this is how we start." Furthermore, the program was to serve as a nodal platform for information exchange and coordination of protective and defensive measures against information technology security incidents against the UN and its related agencies and initiatives (United Nations, n.d.). The DBH brochure (Office of Information and Communications Technology, n.d.) issued by the UN's OICT has identified nine responsibilities of DBH which include uncovering suspicious activities in cyberspace through Big Data and analytics; undertaking

SWOT analysis of UN cybersecurity regime; formulation of cybersecurity strategy for the UN to support its goals; building partnerships and collaboration across the UN on cybersecurity; building capacity to counter current and future threats in cyberspace; building cyber defences beyond firewalls and anti-virus software; building resilience against infrastructure penetration; building digital tools for new ways of cybersecurity and undertaking all efforts through Cyber Operations Centres.

Additionally, the DBH programme is mandated to proactively research and coordinate potential mitigation of at least 19 potential cyber threats (United Nations, n.d.). By doing so, the program is aimed at supporting the UN and its partners in the implementation of 10 out of 17 Sustainable Development Goals (SDGs) (United Nations, n.d.). In terms of managing cyber risks about SDGs and UN Global Compact's Principles, the DBHs have to undertake action in the five areas of focus which primarily include protecting food chains, supply networks and commodities trading markets from cyber-attacks; stopping cyberbullying, exploitation of children, online human trafficking and online illicit trafficking; protecting critical infrastructure, financial markets and institutions from cyber-attacks; preventing cyber corporate espionage, online exploitation, identity theft and financial cybercrime and combating online recruitment of terrorist groups.

The DBH framework comprises of five key action lines, which include help in preventing and combating cyber warfare; protection of critical infrastructure from cyberattacks; facilitating dialogue to ensure a peaceful, open, secure, and cooperative cyberspace; prevent and stop trafficking and online exploitation of people and counter cyber threats to human and economic development (Office of Information and Communications Technology, n.d.).

Materializing DBH's Objectives: Progress and Constraints

Currently, IT professionals and data scientists who work for companies like Google, Amazon, or Tableau are contributing two to three hours of their time to look at problems as part of DBH (Scruggs, 2018). It remains unclear as to how not having a full-time dedicated specialized staff is impacting the functionality of the programme. These professionals have expertise in cybercrime, cyber protection, cybersecurity monitoring. The model which the UN has employed to incorporate their contributions is almost identical to a Code for America model, a model wherein tech and design industry professionals help state and local governments to serve their communities in a better manner (Code for America, n.d.). A review of DBH activities reveals that its current scope of activity is primarily focused on protecting the UN infrastructure (Almutawa, 2020). The program appears to focus primarily on Dark Web and critical infrastructure issues (Akatyev & James, 2017). Additionally, the team has been actively monitoring social media and support projects for achieving SDGs. The programme has built partnerships with several UN entities, including Counter-Terrorism Executive Directorate, Counter-Terrorism Implementation Task Force and UN Women. (Fosse, n.d.).

Moreover, no line of action has been taken so far to protect member states from cybersecurity threats (Dorn, 2017). It was hoped that the UN would be able to assist member states in future once a cadre of cyber protectors is developed (Dorn, 2017). However, no lead has been taken in this regard so far. This is primarily because DBH is not a cyber peacekeeping unit as considered earlier when it was formed (W. Dorn, Personal communication, June 12, 2020).

The five permanent members of the UN Security Council are not interested in allowing the UN to assist member states against cyber-attacks. This is a major strategic objection which prevents the UN from facilitating member states in terms of cybersecurity. However, the incumbent UN Secretary-General has offered his good offices "to contribute to the prevention and peaceful settlement of conflict stemming from malicious activity in cyberspace" (United Nations Office for Disarmament Affairs, 2018, n.d.) through Actions 30 and 31 of the Implementation Plan for Agenda for Disarmament (Implementation Plan, n.d.). Apart from this, an inventory of potential human resources was identified through ITU for undertaking cybersecurity investigations. However, no progress was achieved in this regard (W. Dorn, Personal communication, June 12, 2020).

Some of the activities undertaken by the DBH team include monitoring trafficking of people in the dark web or cryptocurrency and money laundering (Maguire, 2018). In terms of combating terrorism, not much is known except that the DBH team is currently reviewing 'Forensics in a USB stick' solution developed by a team at Singapore Institute of Technology. The solution can be employed for collecting forensic data from computing equipment used by terrorists (Sitizen, 2020).

Along with the UN Office of Information, Communication & Technology Innovation, DBH has been co-hosting the blockchain lab. Like other related agencies, UN Women's work on the blockchain is actively supported by the DBH (UN Women, n.d.). The team has also been working on various applications of Ethereum blockchain (Kryptomoney, 2017). In August 2017, the DBH hosted UN Blockchain Day. The team led a summit in October in New York to speak about how blockchain and other innovative technologies are aiding their humanitarian agenda (Su-Kyong Park, 2017; United Nations, 2017). According to an August 2017 desk review, fifteen United Nations programs were carrying out blockchain initiatives (Starkie, 2017). DBH has also been able to assist peacekeeping operations in terms of securing their online systems and identifying vulnerabilities in their systems through the red teaming approach (W. Dorn, Skype interview, June 12, 2020).

No exact figures are available to suggest the budget allocation of DBH. However, it can be deduced that a very minimal amount is currently being spent on the initiative considering that the UN spends about 6-7 per cent of its budget on information technology (Scruggs, May 2018). Moreover, no details are available to suggest what possible linkages DBH might have with non-UN entities. Considering visible presence of various UN-related initiatives and programs across social media platforms, it is surprising to see that DBH has virtually no presence on social media. A Twitter handle of Digital Blue Helmets (@UN_DigitalBlue) was created in December 2015 (Digital Blue Helmets, 2015). However, the handle has not posted any relevant updates in nearly four and a half years.

Future Outlook and Way Forward

In the long run, the program aims to focus on eight measures: to build the UN's defences against external threats, enrich national cybersecurity defenses for member states, mitigate the effects of 'zero-day' vulnerabilities, establish additional cybersecurity ground rules, promote digital IDs and encourage the shift to biometrics, encourage more robust encryption, combat online trafficking and finally, to improve the ability of the UN to deliver on its mandates through secured ICT (Office of Information and Communications Technology, n.d.).

There is a need for enhanced usage of digital technologies in facilitating peacekeeping operations in future. In this regard, tracking technology could facilitate precision peacekeeping, which will allow for the deployment of most appropriate persons in most appropriate locations. In the near future, the DBH could employ cyber threat hunting and other feasible and ethical means like honey pots, clever decoys and white-hat hackers (Dorn, 2020).

The scope of the DBH program could be expanded in the future to cover an array of related issues of cybercrime and counterterrorism. In order to materialize such efforts, it is essential that additional expertise and resources are available and can be effectively put to use. The team can be complemented with the establishment of a Cyber Peace Corps, built from the Peace Corps and AmeriCorps, in which volunteer cybersecurity professionals would serve clients from all across the world whereas UN cyber peacekeepers would be able to focus on nation-state cyber conflicts. Coupled with Cyber Peace Corps, DBH will have a crucial role to play in managing cyber risks pertaining to SDGs and UN Global Compact's Principles. DBH is expected to focus on cybercrime and primarily cyber-underground marketplaces in the long run (Akatyev & James, 2017, p. 5).

By overlooking the cyber dimension, the UN has reduced the effectiveness of modern peacekeeping operations, which may require cyber intervention. There are several ways in which UN peacekeeping may incorporate cyber component by including protection of the critical information infrastructure of countries (cyber buffer zone); facilitate conflict parties in neutralizing malware; provide IT services to restore the telecommunications and financial system in the post-ceasefire environment; assisting post-conflict countries in transitioning towards stabilization by imparting IT support to local governments by establishing online legal information systems and online education systems (Almutawa, 2020).

Meanwhile, the DBH team could undertake a role that would help with the investigation of a future cyber-attack upon request. A potentially beneficial convergence of interests can be developed between DBH and UN Global Pulse program in terms of data collection and analysis tasks. This collaboration can be helpful in cyber threat detection, prevention and mitigation. However, no details are as yet available, which can imply that such collaboration is either under discussion or is going to materialize in the near future (Akatyev & James, 2017, p. 6). There is also a need for specific allocation within the UN's IT Budget for DBH so that the programme is able to implement its objectives.

The future team composition of the DBH team could include personnel assigned by cyber-contributing countries, cyber-contributing organizations, volunteer experts and UN cyber staff. This team coming from diverse backgrounds could engage in selected projects which are according to their expertise and impartiality. Although it could be challenging to find well-trained and specialized staff from countries and organizations, the UN has been able to overcome such challenges in the past when assembling peacekeeping operations, fact-finding missions and inspection bodies (Dorn & Webb, 2019, p. 22). For fulfilling its challenging mandates, the UN can bring along teams from think tanks and AI-focused institutes and forge a working partnership with DBH. In this way, these teams will be able to have access to the data and resources of the UN's 50-plus agencies and organizations and their domain experts (Smith, 2017).

Using case studies of other UN-related initiatives and programs, the DBH program also needs to work on its social media projection. Currently, the team almost lacks any virtual presence on social media platforms. Likewise, a dedicated website

for DBH program should be allocated, which can act as a one-stop reference for all activities related to the program. The website can also provide a tracker to help in understanding where the program stands in terms of materializing its objectives. This will help in bringing transparency in its operations.

Meanwhile, in order to fully operationalize cyber peacekeeping, it is vital to increase awareness about the concept among UN member states and all across the world. In this regard, more research and consultation will be needed regarding conceptualization, implementation and operationalization of such an initiative. A review of existing scholarship related to the terms 'cyber peacekeeping' and 'cyber peacekeeping' returned thin results; highlighting the dearth of literature. Countries will need to come to support the UN by providing their cyber experts on loan as they have been providing personnel for physical peacekeeping.

Conclusion

Despite the formation of DBH more than four years ago, the program remains in its infancy stage. Several factors appear to have acted as stumbling blocks in keeping the program from completely materializing its objectives. Primary among these blocks is the failure to have specialized onboard staff on a long-term basis for the program. This has had serious consequences regarding the functionality of the program on a prolonged and consistent basis. Secondly, limited budget allocation prevents DBH and other relatable IT projects to harness their full potentials. In addition to the aforementioned challenging factors, failure to adopt a comprehensive strategy regarding the areas that the program envisions to cover have resulted in the uncertain future of the program. Moreover, the uncertainty about its collaboration with non-UN entities prevents the program from achieving its goals with respect to SDGs. Negligible information about its day to day operations result in painting an unclear picture about its current functionality and how it will be able to evolve in future.

The aforementioned issues necessitate a much-needed introspection within DBH regarding whether it is on track to materialize its objectives or not. DBH should have evolved much faster than where it currently stands. It also needs to be more transparent in future (W. Dorn, Personal communication, June 12, 2020). This article can be considered as an exploratory study to look at how DBH has evolved since its formation. Future research studies, depending on availability of literature or access to DBH operations, can understand whether the program is turning out to be a success by formulating some sort of pre-defined criteria to gauge its successes and failures and further explore how the program can potentially play an important role in future.

References

Akatyev, N., & James, J. (2017). United Nations Digital Blue Helmets as a Starting Point for Cyber Peacekeeping. In *European Conference on Cyber Warfare and Security*. 8-16. Academic Conferences International Limited.

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

Almutawa, A. (2020). Designing the Organizational Structure of the UN Cyber Peacekeeping Team. *Journal of Conflict and Security Law*, *25*(1), 117-147.

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.

Code for America. (n.d.). *How We Do It*? Retrieved from https://www.codeforamerica.org/how.

Combating Cybercrime. (n.d.). Retrieved from http://www.combattingcybercrime.org/.

Digital Blue Helmets (@UN_DigitalBlue). (2015, December). Retrieved from https://twitter.com/UN_DigitalBlue.

Digital Cooperation. (n.d.). Retrieved from https://digitalcooperation.org/.

Digital Watch. (n.d.). International Multilateral Partnership against Cyber Threats. Retrieved from https://dig.watch/actors/international-multilateral-partnership-against-cyber-threats.

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

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

Dorn, W. (2020). UN Technology to Cope with COVID and Beyond.

International Telecommunication Union. (n.d.). Global Cybersecurity Index. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

Kenkel, K. M. (2013). Five Generations of Peace Operations: From the "Thin Blue Line" to "Painting a Country Blue". *Revista Brasileira de Política Internacional*, *56*(1), 122-143.

Kleffner, J. K., & 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://digitalcommons.usnwc.edu/ils/vol89/iss1/4/.

Kryptomoney. (2017). 5 Ways How United Nation Sees Potential of Blockchain Technology. Retrieved from https://kryptomoney.com/latest-blockchain-news-united-nations-favours-blockchain-technology/.

LinkedIn. (n.d.). Gudrun Fosse. Retrieved from https://www.linkedin.com/in/gudrun-fosse-2b70484/.

Maguire, Ed. (2018). Podcast #16: Tackling Humanity's Biggest Challenges with Technology, by Atti Riazi. Momenta Partners. Retrieved from https://www.momenta.one/edge/tackling-humanitys-biggest-challenges-with-technology.

Moeda. (2017). Moeda Announces Blockchain Day at the UN: What is "The Blockchain" and its Pioneers. *PR Newswire*. Retrieved from https://www.prnewswire.com/news-releases/moeda-announces-blockchain-day-at-the-un-what-is-the-blockchain-and-its-pioneers-300509514.html.

Nabeel, F. (2019). Establishment of UN Cyber Peacekeeping Force: Prospects and Challenges. *NUST Journal of International Peace and Stability (NJIPS)*, *2*(2). Retrieved from https://www.njips.nust.edu.pk/index.php/njips/article/view/29

Office of Information and Communications Technology. (n.d.). Digital Blue Helmets. Retrieved from https://unite.un.org/digitalbluehelmets/activities.

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

Scruggs, G. (2018). UN IT Chief Atefeh Riazi on the Changing Role of Tech in Development. Devex. Retrieved from https://www.devex.com/news/q-a-un-it-chief-atefeh-riazi-on-the-changing-role-of-tech-in-development-92736.

Sitizen. (2020). *Champions at the United Nations Cybersecurity Challenge*. Retrieved from https://www.singaporetech.edu.sg/sites/default/files/sitizenissue26v2.pdf.

Smith, K. J. (2017). Intelligent Informatics and the United Nations: A Window of Opportunity. The IEEE Intelligent Informatics Bulletin. Retrieved fromhttps://www.comp.hkbu.edu.hk/~iib/2017/Aug/iib_vol18no1.pdf.

Solà Martín, A., & Woodhouse, T. (2011). United Nations and Peace Operations.

Su-Kyong Park. (2017). Blockchain's Potential Leads Future for International Aid. The Stern Opportunity. Retrieved from http://sternoppy.com/2017/10/blockchains-potential-leads-future-for-international-aid/.

Tucci, L. (2016). UN CITO Dreams of Foiling Dark Web with 'Digital Blue Helmets'. *TechTarget*. Retrieved from https://searchcio.techtarget.com/news/4500277224/UN-CITO-dreams-of-foiling-dark-web-with-Digital-Blue-Helmets.

UN Women. (n.d.). *UN-Women's Strategy to Leverage Innovation & Technology to Accelerate Efforts towards Gender Equality and the Empowerment of Women*. Retrieved from https://papersmart.unmeetings.org/media2/18271175/background-brief-unwomens-strategy-to-leverage-innovation-technology.pdf.

United Nations Global Pulse. (2012). *Big Data for Development: Challenges and Opportunities.* Retrieved from https://www.unglobalpulse.org/document/big-data-for-development-opportunities-and-challenges-white-paper/.

United Nations Office for Disarmament Affairs. (2018). *Securing our Common Future: An Agenda for Disarmament*. Retrieved from https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/06/sg-disarmament-agenda-pubs-page.pdf#view=Fit.

United Nations Office on Drugs and Crime. (n.d.). *Global Programme on Cybercrime.* https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

United Nations Peacekeeping. (n.d.). *Mandates and the Legal Basis for Peacekeeping.* Retrieved from https://peacekeeping.un.org/en/mandates-and-legal-basis-peacekeeping.

United Nations Peacekeeping. (n.d.). *Where We Operate*. Retrieved from https://peacekeeping.un.org/en/where-we-operate.

United Nations. (2003). *Handbook on United Nations Multidimensional Peacekeeping Operations.* Retrieved from https://peacekeeping.un.org/sites/default/files/peacekeeping-handbook_un_dec2003_0.pdf.

United Nations. (2017). Bitcoin, Ether, Cryptocurrencies and More. Blockchain Technology Explained @ TechNovation. Retrieved from https://unite.un.org/techevents/blockchain-explained.

United Nations. (2020). *Report of the Secretary-General Roadmap for Digital Cooperation*. Retrieved from https://www.un.org/en/content/digital-cooperation-roadmap/.

United Nations. (2020). *Secretary-General's High-level Panel on Digital Cooperation*. Retrieved from https://www.un.org/en/digital-cooperation-panel/.

United Nations. (n.d.). *Activities*. Retrieved from https://unite.un.org/digitalbluehelmets/activities.

United Nations. (n.d.). *Digital Blue Helmets*. Retrieved from https://unite.un.org/digitalbluehelmets/.

United Nations. (n.d.). *Global Pulse*. Retrieved from https://www.unglobalpulse.org/.

United Nations. (n.d.). Implementation Plan. Retrieved from https://www.un.org/disarmament/sg-agenda/en/#actions.

United Nations. (n.d.). *The Age of Digital Interdependence*. Retrieved from https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf.