Turkish Journal of Science & Technology
16(2), 245-250, 2021

Research Paper

Against Digital Extinction: Cyber Peace

Muharrem Tuncay GENÇOĞLU[*]
[*] Technical sciences Vocational School, Fırat Üniversity, Elazığ, Turkey
[*] mt.gencoglu@firat.edu.tr

(Geliş/Received: 12/07/2021; Kabul/Accepted: 10/08/2021)

Abstract: At a time when cyberattacks are becoming a part of our daily lives and small-scale attacks are becoming commonplace, it is obvious that digital infrastructures are widely and intensely used in our lives and that they can be used for hostile, non-peaceful purposes. This situation has become very serious especially for Turkey, due to the complex attacks taking place around the World.
The issue of cybersecurity around the world is not limited to certain cyberattacks but also brings the threat of these attacks turning into comprehensive cyber warfare. Therefore, the more important the security of the geographical borders, the more important the security of electronic systems and the data stored there. Since the most important component of security is peace, it is worth examining as a very important concept in Cyber Peace in response to the negative perceptions of cyberwar, cyber terrorism and cybercrime. This study, it is aimed to create a conceptual basis of cyber peace and contribute to this field to create a defense mechanism based on peaceful behaviors in cyberspace. For this purpose, the definition of cyber peace has been made, and it has been focused on establishing and protecting cyber peace. It was emphasized that cyber peace can be sustainable not through disarmament, but by reducing the risk through modernization of attack and defense capacities.
In this study, which we do not have much work on cyber peace and we can accept it as the first step in filling this gap; It was concluded that private and voluntary organizations must take a more active role in protecting cyber peace.

Key words: Peace, Cyber Peace, Cyber Peace Protection, Cyber.

Dijital Yokoluşa Karşı: Siber Barış

Öz: Siber saldırıların günlük hayatımızın bir parçası haline geldiği ve küçük çaplı saldırıların sıradanlaştığı bir dönemde, dijital altyapıların hayatımızda yaygın ve yoğun bir şekilde kullanıldığı ve düşmanca, barışçıl olmayan amaçlar için kullanılabileceği aşikardır. Bu durum, dünya genelinde yaşanan karmaşık saldırılar nedeniyle özellikle Türkiye için çok ciddi bir hal almıştır. Dünya genelinde siber güvenlik konusu belirli siber saldırılarla sınırlı kalmayıp, bu saldırıların kapsamlı bir siber savaşa dönüşme tehdidini de beraberinde getiriyor. Dolayısıyla coğrafi sınırların güvenliği ne kadar önemliyse, elektronik sistemlerin ve orada depolanan verilerin güvenliği de o kadar önemlidir. Güvenliğin en önemli bileşeni barış olduğu için siber savaş, siber terörizm ve siber suçlara ilişkin olumsuz algılara karşılık Siber Barışta çok önemli bir kavram olarak incelenmeye değerdir. Bu çalışma ile siber barışın kavramsal bir temelinin oluşturulması ve bu alana siber uzayda barışçıl davranışlara dayalı bir savunma mekanizması oluşturulmasına katkı sağlanması amaçlanmaktadır. Bu amaçla siber barışın tanımı yapılmış ve siber barışın kurulması ve korunması üzerinde durulmuştur. Siber barışın silahsızlanma yoluyla değil, saldırı ve savunma kapasitelerinin modernizasyonu ile risklerin azaltılması yoluyla sürdürülebilir olabileceği vurgulanmıştır. Siber barış konusunda çok fazla çalışmamızın olmadığı ve bu boşluğu doldurmanın ilk adımı olarak kabul edebileceğimiz bu çalışmada; Siber barışın korunmasında özel ve gönüllü kuruluşların daha aktif rol alması gerektiği sonucuna varılmıştır.

Anahtar kelimeler: Barış, Siber Barış, Siber Barışı Koruma, Siber

1. Introduction

We are in a period where cyber attacks are becoming a part of our daily lives and small-scale attacks are becoming commonplace. It is obvious that digital infrastructures entered our lives extensively and intensely during this period and it is inevitable that they will be used for hostile and non-peaceful purposes. We have witnessed quite complex attacks around the world. The issue of cybersecurity around the world is not limited to certain cyberattacks but also brings the threat of these attacks to turn into comprehensive cyber warfare. Therefore, the more important the security of the geographical borders, the more important the security of electronic systems and the data stored there. Since the most important component of security is peace, it has taken its place in the literature as a very important concept in Cyber Peace in response to the negative perceptions of cyberwar, cyber terrorism and cybercrimes. For this reason, it is important to create a conceptual

[*] Corresponding author: mt.gencoglu@firat.edu.tr. ORCID: 0000-0000-0002-8784-9634

basis of cyber peace and contribute to this field to create a defense mechanism based on peaceful behavior in cyberspace.

The World Federation of Scientists has placed the concept of Cyber Peace at the center of its studies for the last few years, and the International Telecommunication Union (ITU) has been striving to make the concept more concrete with its recent and supported studies. One of the steps taken to ensure cybersecurity in the international arena is the "Paris Call for Trust and Security in Cyberspace" signed in November 2019. Among the supporters of the agreement, the majority of which are private sector organizations, are 67 states as well as 139 international institutions and non-governmental organizations. Although it is a comprehensive and positive step in the field of cybersecurity, the fact that countries with strong cybersecurity infrastructure such as the United States, Russia, Britain and Israel have not signed the agreement, the agreement has the nature of a declaration and the lack of sanction power raises questions about its effectiveness, but civil society is involved in the issue. It is of vital importance for the future of the subject.

The most striking developments in the field of cyber peace are; There are foundations and organizations established to ensure security in the cyber world. One of the last examples of initiatives developed against cyberattack threats is the Cyber Peace Institute, which was established in Geneva in September 2019. Established under the leadership of technology giants such as Microsoft, Hewlett Foundation and MasterCard, the main purpose of the institute is to make the internet a more stable and secure space. Although it was founded by the aforementioned technology giants, the institute is completely independent and set out with the slogan "Towards a safer online world for all", the institute's main strategies include helping civilian victims of cyber attacks, investigating and analyzing cyberattacks In addition to ensuring the establishment of international laws and norms in the field of cybersecurity. Declaring that it will support civilians who are in the most vulnerable position against cyber attacks, the institute will fill this serious gap in the field.

One of the few organizations working on cybersecurity is the Cyber Peace Foundation of India. I guess it would not be wrong to say that the foundation is the most active non-governmental organization in the field. The Foundation is a very successful example of a social enterprise model in the field of cybersecurity, with its work in different fields. Founded in 2013 under the leadership of a young entrepreneur, Vineet Kumar, the foundation conducts international studies in addition to India and also produces its policies based on the Sustainable Development goals of the United Nations. Kumar defines the foundation's main founding purpose as “to create a civil society movement against the proliferation of state-sponsored cyber attacks and cyber weapons”[4]. Cyber Peace Alliance and Cyber Peace Corps are two of the foundation's most important initiatives. The alliance, established in partnership with the Indiana University Ostrom Workshop, the Cyber Security and Internet Governance Program, and the Cyber Peace Foundation, was established to look at the concepts of cyber peace and cybersecurity from an interdisciplinary perspective and to conduct various researches. The Cyber Peace Union is a network of volunteers of the foundation and is called the "Volunteers Battalion" by Kumar. These volunteers work to help people of all ages who need cybersecurity in different areas[4].

In addition to these initiatives; Two initiatives such as the Cyber Security Technology Agreement (Cyber Security Tech Accord), signed under the leadership of Microsoft, and the Charter of Trust, which was initiated under the leadership of Siemens and signed during the 2018 Munich Security Conference, can be mentioned as important developments in this field.

Nations should try to reduce the emerging cyber arms race by establishing a foundation of trust. The international community has taken useful steps in this direction, for example, with the European Convention on Cybercrime, the UN report on cybersecurity that requires a series of actions to make information infrastructures more secure.

1.2. Literature Review

When the subject is scrutinized academically, there are quite a few valuable studies;

In Bloom and Saveg's studies; They emphasized that focusing on reducing national and international risk while discovering all cyber capabilities would be the best deterrent method against cyber conflict[5]. As Akatyev; emphasized the need for cyber peacekeeping and defined cyber peacekeeping goals[6]. Lynn emphasized the complexity and rapidly changing environment of cyberspace, highlighting the importance of coordinated and rapid response to threats for cyber peace [7]. Cahill, et al. Analyzed some principles, possible applications and technologies of cyber peacekeeping [9]. Kleffner and Dinnis examined the international legal aspects of cyber activity in cyber peacekeeping operations[10]. Şahin examined cyber peace as an alternative concept in the light of liberalism and realism[11].

2. Peace

Peace is not an unattainable goal; rather, it is a negotiation between the rights, lives, well-being and safety of each individual concerning others. This is not a hard-won war either, for then it would be the imposition of someone else's will on another, and that would be victory, not peace.

Generally, the concept of peace is interpreted both positively and negatively. On the positive side; It means good governance, regular resolution of conflict, harmony, gentleness and love. On the negative side; the absence of anything means the absence of chaos, tension, conflict and war [2]. By achieving positive cyber peace and eliminating structural forms of cyber violence, many of the challenges today can be addressed.

In the creation of a culture of peace and peace, not only the use of force and non-violence but also a common set of values, behavior patterns, laws, positive-dynamic-participatory processes should be established in the international arena. It is also vital to promote freedom, justice, democracy, tolerance, solidarity, cooperation, pluralism, cultural diversity, dialogue, understanding and conflict resolution. It is particularly important to create a cyber context in which the preconditions for peace, such as respect for everyone's right to freedom of expression, opinion and information, are particularly important, as well as the much-emphasized moral aspects of peace.

When viewed from this angle; Instead of finding another analogy of "what cyberspace looks like" or discussing how much individuals or firms can "back down", it would be better to start by examining the structure of cyberspace, and the types of violence that can occur in and through cyberspace. Only in this way is it possible to solve problems at their source. With the concept of Cyber Peace, the establishment of the universal order of cyberspace is aimed at as the basic principle. However, a basic definition still needs to be made.

In August 2019, the World Federation of Scientists, based on the Erice declaration, which determines certain actions and obligations to ensure peace and stability in the cyber field, determined the basic operational elements of cyber peace as follows;

1. The free circulation of information and ideas guaranteed by international law to individuals also applies to cyberspace. Restrictions should be within the legal process and to the extent necessary.
2. All countries should work together to develop a common code of cyber conduct and a harmonized global legal framework, including provisions on judicial investigation cooperation that respects confidentiality and human rights.
3. All users, service providers, and governments should work to prevent the use of cyberspace, especially young and vulnerable users, in a way that could lead to violence or exploitation.
4. The private sector, including governments, organizations, and individuals, should implement and maintain comprehensive security programs that leverage privacy and security technologies based on internationally accepted best practices and standards.
5. Software and hardware developers should strive to improve resilience and develop secure technologies that are resistant to vulnerabilities.
6. Governments should actively participate in the efforts of the United Nations to support global cybersecurity and cyber peace, as well as prevent the use of cyberspace for conflict.

If the concept of cyber peace is taken seriously, first of all, a legal framework should be determined to define what violates peace. They must undertake that they will not launch the first cyberattack and will not go unpunished by the cyber terrorists and attackers in their country. In addition, these commitments can include non-attack on critical national infrastructures, particularly those that serve basic humanitarian needs, and the inviolability of cross-border data networks. However, to be realistic; Such strategies and principles designed to promote cyber peace are likely to be sabotaged by countries with cyberwar potential. It will create distrust for other countries. At this point, when the current reports such as the systematic armament of cyberspace and the development of cyber-attack strategies are examined, the trust environment is problematic. Therefore, decisive enforcement action is needed to contribute to cyber peace, cyber stability and fundamental rights.

Cyber peace; aggression, counterattack, and retaliation should not be completely indispensable but should include feasible scenarios. The keyword here should be a restriction. A rigorous, ongoing threat and risk analysis should be carried out to prevent uncontrollable consequences, including the careful protection of humanitarian and socially indispensable critical infrastructures.

It is necessary to define cyber peace from both aspects of peace. Because we cannot define it simply by the absence of conflict and war; The reason is that these elements are not seen in the digital space. Therefore, in cyber peace, it is necessary to define the stable peace zone first. The region where peace is maintained based on mutual and consensus is called a stable peace zone. Sustainable, safe and flexible systems should be established to ensure peace in this region.

For the time being, a peaceful situation in cyberspace does not seem possible. However, if cooperation and trust between actors can be increased, a positive atmosphere can be created towards a stable peace environment. Action should be taken to stabilize cyberspace and reduce the potential effects of hostile actions.

Cyber peace can be achieved. Since human beings have created technology, human beings can find technological solutions to certain problems themselves. Man can find humane solutions to his problems. Cybersecurity and cyber peace are two sides of the same coin and should therefore be handled together.

2.1. Cyber Peace

It is a universal cyberspace order built on a healthy state of peace, disorder or discomfort and the absence of violence [1].

The International Telecommunications Union (ITU) has accelerated the work by pioneering some of the first studies in this field by defining cyber peace as a "universal cyberspace" system built on a "healthy state" in part. Based on these studies, we can define cyber peace as follows;

It is a regime that respects human rights, spreads internet access with best practices, promotes multi-stakeholder cooperation and prepares the ground for reducing the risk of cyberwar with a new cybersecurity approach that strengthens governance mechanisms.

Based on this definition; By helping to reduce the threats of cyber conflict, crime and espionage to comparable levels, by making clear the rules for companies and governments, it is possible to say that a multilevel network of regimes that promotes global, fair and sustainable security can only be built with cyber peace.

2.1.1. Ways to Achieve Cyber Peace

Although it seems unlikely that cyber warfare and conflicts can be prevented completely soon, it may be possible to reduce the likelihood and impact of conflicts and to move from a negative peace state to a stable state of peace. Namely;

- This Will lead to some degree of restriction on the attack as all stakeholders are interconnected
- Internet protocols are in place and will contribute to peace as they are widely accepted.
- The presence of defense organizations trying to increase Internet security and stability will contribute to the formation of a peaceful environment as it will provide an advantage in forming supranational groups.

Their offensive capabilities are also a deterrent in maintaining a stable peace. Because the attacker is afraid of retaliation, defensive measures reduce the likelihood of a successful attack. The two most important components of a stable cyber peace are flexible security and trust.

Technically flexible security is the most important factor that helps reduce the likelihood and impact of digital attacks. The higher the impact of this factor, the more reliable the infrastructure will be. Trust is an important component of collaboration for actors in the digital space. Based on security and trust, it is possible to exclude the risk of attack against government primary attacks. Because there are protocols, processes and agreements that create stable peace [2].

It is time to make critical decisions to change the world's cyber defense approach and provide viable solutions to the challenges it faces in cyberspace. For this reason, raising awareness of all individuals in the field of cyber peace requires the efforts of all sectors. On the other hand, there is a need for international and binding legal regulations that will prevent cyber attacks from being instrumentalized by states. Civil society has to undertake important tasks to create the necessary pressure tools for this to happen.

Establishing and maintaining cyber peace can be as challenging as starting a cyberwar. Because defining and promoting cyber peace is not as easy as it seems. However, all stakeholders should engage in a constructive dialogue, harmonizing different approaches to governance and ensuring a collaborative environment that is critical to achieving a point between internet sovereignty and freedom that both respects human rights and guarantees vital systems. However, by preparing the ground for cyber peace with these initiatives, cyberwar can be stopped before it starts [3].

3.Cyber Peace Protection

Cyber Peace Preservation is essential to protect an increasing number of people in cyberspace, establish inter-state arbitration to help prevent the escalation of cyber conflicts, and help build and maintain trust and openness.

Cyber Peace Protection is defined as rehabilitation that focuses on civil security by preventing, mitigating, later limiting and mitigating cyber conflict [6].

Cyber Peacekeeping works to promote online safety and security following international laws and treaties, whose main purpose is to protect civilians. A framework should be put forward to maintain permanent conditions of peace in cyber and physical areas affected by potential threats in cyberspace. Certain roles should be defined at different stages of peace conditions.

Each role of Cyber Peacekeeping can contribute to the safety and security of cyberspace at three different stages of a conflict, the absence of conflict, during and after conflict. Namely; monitoring potential threats when there is no conflict. It can be explained as stopping the spread of cyberattacks during conflict and as a last measure the creation of cyberweapons that respond with counter-attacks [8]. The relationships between roles, goals, and functions are shown below (Fig. 1).

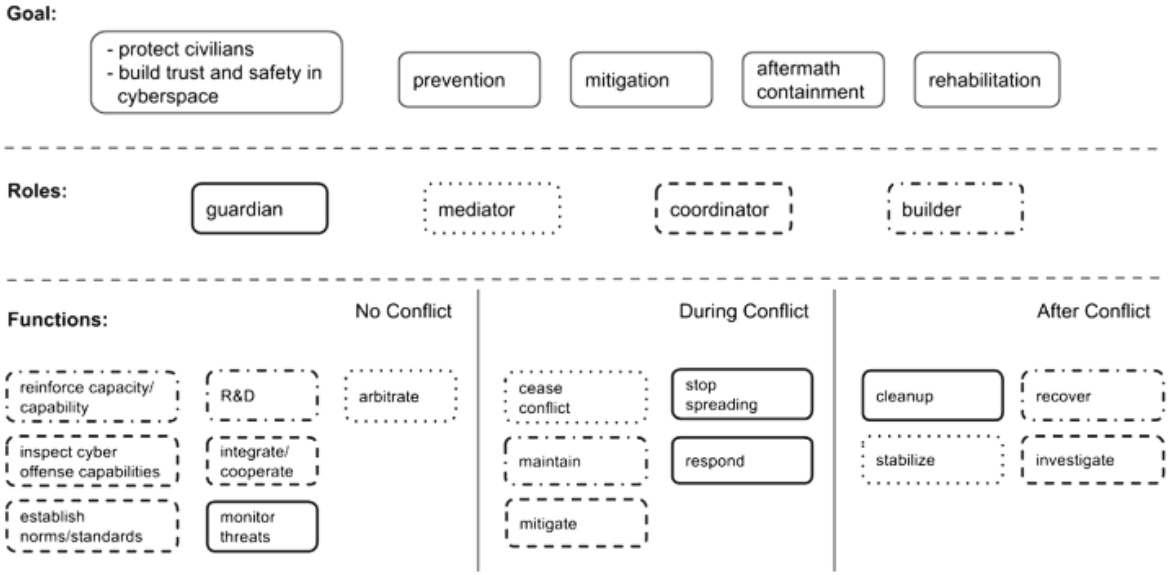

Fig. 1. Different stages of the conflict in cyber peacekeeping and the relationships between them [6]

We can say that there are generally eleven different activities carried out in the UN peacekeeping operation [12]. These activities are shown in the figure below (Fig. 2). Peacekeeping operations are the practical measure by which the UN fulfills this task and is the rationale for establishing peacekeeping operations [8]. If cyberwar threatens international peace and security, the UN should act on peacekeeping duty.

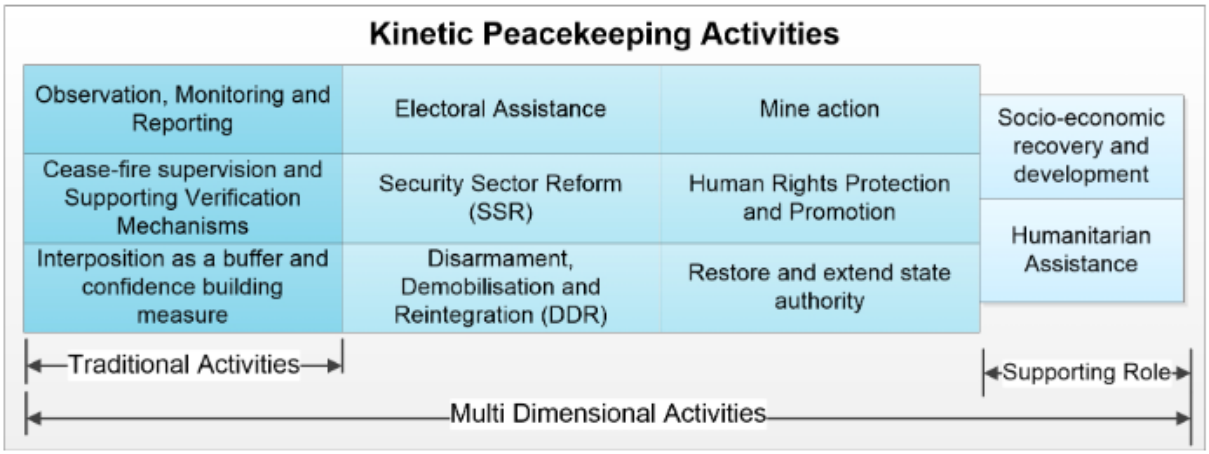

Fig. 2. Peacekeeping activities [13]

Cyber peacekeeping will be necessary for the future, and it is now important to define what cyber peacekeeping means. This is not simple, as to how to define peacekeeping is a constant source of debate [8]. To simplify the work, we can take the definition of the UN made; "The action taken in places where the conflict is

stopped to preserve the peace, even though it is fragile, and to help implement the agreements reached by the peacekeepers"[14].

3.1. The Challenges of Keeping Cyber Peace

Several challenges will be faced in maintaining cyber peace. However, it is necessary to consider both technical and political difficulties. It would be worth further researching the potential for resistance and how to overcome it.

Providing the required number of peacekeepers is a challenge in itself. Today's UN operations are carried out with the contribution of full-time UN staff and soldiers and experts from UN member states. However, it is also necessary to evaluate resources such as cybersecurity experts from the private sector and voluntary organizations.

There are probably many more obstacles. Each activity concluded to be necessary and feasible requires further investigation to discover where the additional barriers are and how to resolve them.

4. Conclusion and Recommendations

As a first step in reducing the risk of conflict, each country should make an internal assessment of their exposure to attack. First, critical infrastructure areas need to be studied thoroughly and clearly. Second, steps must be taken to improve the security of hardware and software. Third, it is necessary to work with other countries to share knowledge and establish norms of behavior, especially in times of crisis.

Cyber peace can be sustained not through disarmament, but risk reduction combined with the modernization of each rival country's attack and defense capacity. Organizations and individuals who believe that maintaining the status quo is in their interest will pose significant obstacles to reducing cyber risk. Innovative mechanisms will be required to overcome this organizational and individual resistance. Organizing these mechanisms around principles of behavior such as amnesty, community, internal transparency, competition, globalization, enforcement and international norms would be a good model for the change required to secure cyberspace. As this model requires extensive cooperation, states should be held directly responsible.

Cyber peacekeeping is a very difficult issue, but the fact that cyberspace hosts activities such as terrorism, espionage and war reveal the need for a practical solution. Cyber Peacekeeping is still a new and untested idea. Future work should be shaped by feedback from potential stakeholders.

While there is no need to maintain cyber peacekeeping today, it is clear that it will be needed shortly as cyber warfare becomes more common. Since operating in cyberspace will be an increasing necessity to keep the peace, official, private and voluntary organizations should take a more active role.

For Cyber Peace, you need to be ready for Cyber War!

References

[1] Hamadoun, I. T. The Quest For Cyber Confidence, 77, 2011.

[2] Inversini, R. Cyber Peace: And How It Can Be Achieved, The Ethics of Cybersecurity, Christen, M., Gordijn, B. ve Loi, M. (Ed.), 259-276, 2020.

[3] Shackelford, S. J. Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Cambridge University Press, 2014.

[4] Çakır, M. N. Siber Güvenlik İnisiyatifleri ve Sivil Toplum, 2019. https://www.sivilsayfalar.org/tag/siber-baris-enstitusu/

[5] Bloom. L. Savag, J. E. On Cyber Peace. Atlantic Council, 2011.

[6] Akatyev, N. Cyber Peacekeeping, Digital Forensics and Cyber Crime, 126-139, 2015.

[7] Lynn III, W. J. Defending a new domain: the pentagon's cyber strategy. External Affairs, 89, 97–108, 2010.

[8] Bellamy, A. and Williams, P. Understanding Peacekeeping. Polity, 2010.

[9] Cahill, TP, Rozinov, K., Katır, C .: Cyber Warfare Peacekeeping, s. 100. In: Proceedings of the 2003 IEEE Workshop on Information Assurance, 2003.

[10] Kleffner, JK, Dinnis, H.H. A. Cyber peacekeeping: international legal aspects of cyber activity in peacekeeping operations. International Law Studies. 89, 1, 2013.

[11] Keskin, Ş. Realizm Ve Liberalizm Işiğinda Siber Savaş Ve Alternatif Bir Kavram Olarak Siber Bariş'in Değerlendirilmesi, TURAN-SAM Uluslararası bilimsel dergisi, 9(35), 287-297, 2017.

[12] United Nations, United Nations Peacekeeping Operations: Capstone Doctrine.January 2008.

[13] Robinson, M. Jones, K. Janicke, H and Maglaras, L. An Introduction to Cyber Peacekeeping, Senior Member, IEEE, 2017.

[14] Mays, T. Historical Dictionary of Multinational Peacekeeping. Scarecrow Press, 2010.