The Role of Nato in Enhancing Ukraine's Cybersecurity during Times of Conflict

Dewi Triwahyuni[1*], Leonardo Valentino[2], Nenden Nurmutiasari Amada[3], Harya Bustami[4]
[1,2,3]Departement of International Relations, Universitas Komputer Indonesia, Indonesia.
[2]Departement of International Relations, Universitas Komputer Indonesia, Indonesia.
[4]Information Systems, STMIK Kaputama, Indonesia

Abstract. This study aims to analyze the impact of NATO support on Ukraine which is in a conflict situation with Russia. Ukraine has taken a step forward to strengthen its ties with NATO by signing an agreement to formalize its participation in the security alliance's Joint Center for Advanced Technologies in Cyber Defense (CCDCOE). This study will discover how this action will affect the tensions in the Cyber Security System between Ukraine and Russia. In order to find the answer, it is necessary to identify the motives by using qualitative research design through secondary sources in the form of official state documents and secondary sources in the form of journals, dissertations and related research. The result of this study conluded NATO's involvement in the cyber war between Ukraine-Russia is quite substantial and greatly influenced the course of the war, this is what motivated the researcher to conduct further studies and see what influences were given., regardless of the difficult to collect the information. This study might help us understand the situation of Cyber Conflict between Ukraine-Russia and predicts the potential consequences from this action, and hopefully give us more informations to analyze and evaluate to find the best solution of this existing conflict.

1. Introduction

In reaction to expansive scale assaults to its basic foundation, Ukraine embraced a National Cybersecurity Procedure and making strides in its execution, The setup of the National Cybersecurity Coordination Middle in 2016 and the proposed overhaul of the cybercrime enactment to meet the Budapest Tradition necessities and best hones, especially on Web Benefit Suppliers, are a few primary steps in improving the country's cyber strength. These exercises are complimented by solid participation with worldwide accomplices over the cyber circle, counting on cybercrime and cyber defense. Russian operations in cyberspace have largely gone unnoticed in recent years due to acts by the cyber security sector, or so-called "patriotic hackers," who

have taken it upon themselves to oppose Russian cyber aggression and target Russian cyber infrastructure. US and Western European commentators projected terrible and debilitating cyber repercussions based on kinetic warfare with the Russian invasion of Ukraine in 2022. The North Atlantic Treaty Organization (NATO) should evaluate and formulate a policy for collective cyber defense in light of such developments.

Globally, cyberspace has spread, especially in critical infrastructure, as technology has surpassed conventional notions of computing. Non-traditional computers can make phone calls, fit in pockets, and are becoming capable of taking high-quality pictures. These non-conventional computers also keep food at the appropriate temperature in kitchens, provide instructions in automobiles, and monitor activity and health on wearable devices worn by individuals. But more significantly, these unconventional computers are found at critical infrastructure hubs where they provide data to operators through enormous screens mounted on walls and closed-circuit video cameras that depict the actual surroundings. Many of these devices, which typically don't have anti-virus software and use weak protocols, are either already present in vital infrastructure or have been carried in by workers. Water, telecommunications, finance, and the production and distribution of electrical power.

The inclusion of Ukraine in the CCDCOE will improve the sharing of cyber experience between Ukraine and the organization's member states. Additionally, this is a significant step towards Ukraine joining NATO because of SSSCIP's involvement in the CCDCOE proposal that was submitted by Ukraine in August 2021. The Steering Committee members unanimously approved Ukraine's membership on March 4, 2022. Ukraine membership in the CCDCOE will be formalized once the Technical Agreement on Accession is signed by Ukraine and the remaining CCDCOE members. The NATO Cooperative Cyber Defense Centre of Excellence is a key NATO institution for cyber defense, addressing cybersecurity-related issues at both the strategic and practical levels. 25 NATO Allies and 4 partner states make up the Center.

Recent state actions show how cyber operations may have negative physical effects. Iran attempted to overchlorinate Israeli water treatment facilities in the summer of 2020, turning faucets into poison distributors. More recently, in February 2022, Russian assaults on Viasat satellite networks affected German windmill energy generation and distribution in an effort to sever communications within Ukraine. Furthermore, Russia has targeted electrical power generating and distribution networks in the past and is continuing to do so in the ongoing conflict as recently as April 2022, harming Ukrainian military and civilian infrastructure.

The Major Formulation of The Problem in this research is what exactly the impacts of NATO involvements on this existing conflict, is there any political interest by NATO on helping Ukraine which is has improved the Cyber Security. In order to find answers to the researcher's questions, we need to formulate the right problem in order to get satisfactory results and information that is also useful in providing answers to the problems that have been studied, in this case cyber security is something that is not conventional so it is rather difficult to identify the perpetrators of cyber attacks, but if viewed from a political point of view, of course all actions have a certain purpose, in formulating the problem we will see how NATO's involvement in strengthening Ukraine's cyber security. and how Russia responds to NATO and Ukraine's cooperation.

To measure the extent to which this paper can be influential, researchers must look at previous writings or research related to NATO's involvement in strengthening Ukraine's cyber defense, in this case, researchers have found 4 literature studies that are similar to this research. *First* research, is written by M. Yusuf Samad [1] : Understanding Russian Cyber Warfare and the Role of the State Intelligence Agency in Countering Cyber Threats. This study focuses on cyber attacks that took place in Georgia, Estonia and Ukraine. The attacks were able to paralyze vital infrastructure in both countries. Similar attacks could potentially take place in Indonesia, so it's important to understand the mechanics of cyberattacks and how

to prevent them. This study uses a qualitative approach and the research goal is to understand the cyber attackRussian Cyber War with Estonia, Georgia and Ukraine. This study tooaims to understand the role of the National Intelligence Agency in countering cyber threats in Indonesia.threats in Indonesia.The results of this study are that cyber attacks on Georgia, Estonia and Ukraine are carried out in every phase of cyber early warning. Preventing Similar Attackssimilar attacks, BIN plays a role in countering cyber attacks by coordinating intelligence, cyber patrols and security assessments. The Different between this Research and our research is the NATOs involvement which is more exposed in our research. and focus on the impacted of this action[2]. Reseach from Ujang Priyono : Cyber Warfare as a part of Russia-Ukraine War [2]. Russia and Ukraine have had strained relations since 2014 that have led to acts of violence. Cyber attacks have become part of this conflict, as well as border issues and the separatist movement in Ukraine. Tensions between the two countries increased in 2021, and in early 2022 there was a major cyberattack on the Ukrainian government's website. Claiming that Russia was the mastermind behind the cyberattack, the Ukrainian government has escalated the feud between the two countries. Starting from the time of wars and cyber attacks related to Ukraine, this study aims to examine the connection between cyber attacks and the political policies of the two countries in the face of the conflict.The cyberspace dilemmas of finding evidence that real cyber attackers exist are also detailed. The Similarity is the cyber war between Russia and Ukraine but the different is the involvement of NATO and impact. [3]. Research written by Made : The Role of UN as an International in The Conflict of Russian-Ukraine

This study examines a world concerned about tensions between Russia and Ukraine that began late last year. Tens of thousands of Russian troops were initially stationed on the Ukrainian border. In the wake of NATO and US actions, tensions began to rise and the crisis was bound to escalate. The article discusses the role, purpose and function of the United Nations in conflict resolution and its influence in achieving that solution, as the United Nations has an important responsibility in finding a solution to this problem. This article uses a normative legal construction as the data comes from literary sources of related articles and books.The UN should play an important role in this matter as a mediator who can find solutions for both sides, because the UN is the largest international institution. Since Russia has a right of veto over these resolutions, it can be said that the consequences of the UN resolutions are useless. this Research is aim to inform the impact of UN in this conflict, while our research is focusing to study the NATO role in this conflict.[4]. Research written by Rohman : Russia-NATO Rivalry and Strategic Influence in Eastern Europe on Security and Economy

Growing global powers such as NATO, the European Union, China and Russia have different characteristics and interests in world politics. Russia after the collapse of the Soviet Union tends to be in a relatively weak position in terms of influence, security and economy. Today, Russia's relations with the European Union and the United States have improved after the Cold War. In recent years, Russia and NATO have not only strengthened their economic and military-related security, but have gone further to strengthen their main influence in Eastern Europe. This study will examine Russia's political policies towards NATO and Eastern Europe from the perspective of security and economic interests. The method used is qualitative by conducting an in-depth study of data obtained from previous research results. The results of this study indicate that Russia and NATO are involved in competition for strategic influence in Eastern Europe, especially Ukraine and the former Soviet Union. Russia and NATO, sponsored by the United States, are trying to achieve their respective interests by making efforts to increase power which includes political, security and economic power.[5].Research from Rum : Practical Use of Cyber Operation (CYBER WARFARE) In Conflict Armed Conflict from the Perspective of International Humanitarian Law
This research aims to find out the position of cyber operation in

armed conflict and cyber warfare methods through the perspective of international humanitarian law, as well as the form of protection provided to perspective, as well as the form of protection given to civilians in cyber warfare by international humanitarian law.

This research is a normative research where the sources are processed using the interpretation method. The legal materials used consist of primary legal materials namely related conventions, as well as secondary legal materials obtained from books, journals, and related documents. The results of this study, namely international humanitarian law does not have binding legal instruments to date regarding cyber operations and cyber warfare. Nevertheless, international humanitarian law can still apply when cyber operations are used on the condition that the impact caused by the operation is equivalent to the impact that can be caused by kinetic operations. International humanitarian law provides protection for civilians in cyber warfare as well as from cyber operation attacks as long as the civilian does not perform an action that is considered as direct participation in combat.

This research collects some information from several previous studies such as the research above to compare how this research can provide new information related to the cyber war between Russia and Ukraine and how NATO is involved in this conflict and also to have a good view of the current problems in Ukraine by using the qualitative method such as information gathering through interviews, news and literature studies to analyze the issues using expert theories, conclude actions, and provide accurate results.

2. Research Method

This research will be using the qualitative research method to have better understanding regarding the Role of NATO in the conflict of Russian and Ukraine. The author used qualitative research method in order to explore, analyze, and explain the connection between the theory and the research topic. This paper used qualitative analysis methods that are written based on primary, secondary and tertiary literature review that include speech text, primary report, e-book, academic articles, think tank review dialogues, newspaper, official website and handbooks. At the end of the research, authors will find result from analyzing the theory. as NATO policy to support Ukraine by suggeting Ukraine to be a participant in CCDCEO.Ukraine has taking more step forward by joining this NATO's defence group and the qualitative method is the most reliable method to analyze the motives behind this cooperation and why Russia has insisted to revoke the cooperation between NATO and Ukraine through secondary sources in the form of official state documents and secondary sources in the form of journals, dissertations and related news on website.

3. Results and Discussion

3.1 The Cyber Security Strategy of Ukraine

Approved on March 15, 2016, by Decree of the President of Ukraine, identifies cybersecurity risks and the corresponding goals for maintaining Ukraine's cybersecurity. This document, which is based on the requirements of the Council of Europe Convention on Cybercrime, intends to provide the necessary frameworks for the secure operation of the internet and the responsible use of it by individuals, society, and the government. The first official report in the field of cybersecurity was published by Ukraine in 2016. Along with the conventional "Earth," "Air," "Sea," and "Space" spheres of hostilities, it acknowledges "Cyberspace" as a distinct area of hostilities in which the necessary units of the armed forces. [6]

The second iteration of Ukraine's state security strategy, adopted by presidential decree in September 2020, became the basis for several new initiatives in various sectors. The development and security of cyberspace, the implementation of e-governance, guarantees of security and long-term functionality of communications, and national information resources should become an integrated part of Ukraine's state policy on the growth

of the information society and the development of information space. the following are the three guiding principles of state policy in the field of national security that form the basis of the strategy :

1. To prevent violent attack against Ukraine, deterrence, security, and defense capacities must be developed.
2. Resilience is the capacity of a community or a state to swiftly adjust to changes in the security environment and continue sustainable operation, particularly through reducing external and internal vulnerabilities.
3. To engagement, development of pragmatic collaboration with other nations and international organizations based on Ukraine's national interests, and the development of strategic ties with important foreign partners, especially the European Union, NATO, and their member states, the United States. [7]

3.2 Russian's Cyber Attacks on Ukraine

Russia's invasion of Ukraine began on February 24, 2022, but since its illegitimate acquisition of Crimea in 2014, Russian cyberattacks have continued and become more severe. The public, energy, media, financial, commercial, and nonprofit sectors in Ukraine have suffered the most during this time. Numerous cyberattacks from Russia have hampered the transportation of medical aid, food, and humanitarian supplies since 2013. Their effects have included data theft and deception, notably through the use of deep fake technology, in addition to restricting access to fundamental services. Phishing emails, distributed denial-of-service attacks, data-wiper malware, backdoors, surveillance software, and information thieves are some more hazardous online activities[8]. Here are a few Russian's Cyber Attacks on Ukraine:

1. Operation Armageddon
   Russia's invasion of Ukraine began on February 24, 2022, but since its illegitimate acquisition of Crimea in 2014, Russian cyberattacks have continued and become more severe. The public, energy, media, financial, commercial, and nonprofit sectors in Ukraine have suffered the most during this time. Numerous cyberattacks from Russia have hampered the transportation of medical aid, food, and humanitarian supplies since 2013. Their effects have included data theft and deception, notably through the use of deep fake technology, in addition to restricting access to fundamental services. Phishing emails, distributed denial-of-service attacks, data-wiper malware, backdoors, surveillance software, and information thieves are some more hazardous online activities.. The purpose of the strikes was to give Ukraine an advantage in kinetic combat. The CTIG has discovered evidence linking waves of Operation Armageddon with Russian military operations in and around Ukrainian war zones through intensive temporal and technological analysis. It is obvious that Russia is still developing its information warfare components as part of its broader modern warfare methods in order to promote its international objectives. [14]

2. Operation Snake
   A cyber espionage "tool kit" called Snake, which resembles a system that plagued the Pentagon several years ago and attacked classified systems there, has been infected for years by dozens of computer networks in Ukraine, according to a report released by the British defense and security company BAE Systems. As the protests in Kiev intensified this year, the virus surfaced far more

often in Ukraine. The refusal of Yanukovych to pursue greater political and economic relations with Europe, which has been competing with Russia for influence in Ukraine, infuriated the demonstrators. According to the BAE paper, the snake, also called Ouroboros after the serpent in Greek mythology, grants attackers "complete remote access to the infected system." According to BAE, there is some Russian content in the code and the malware creators work in the Moscow time zone, providing circumstantial proof that the assaults originated in Russia.[15]

3. Attacks on the automated system "Elections" 2014
   Additional malware was discovered on the electoral commission's system, according to a Ukrainian official looking into the event who spoke to NBC News on the condition of anonymity because the investigation into the incident is ongoing. This was related to the APT28 gang, also known as Fancy Bear, which has been implicated in recent hacking incidents in the United States. Although the 2014 incident did not affect the results of the elections in Ukraine, the hackers succeeded in their purpose of undermining the election, Viktor Yanukovych, a pro-Russian politician, had been ousted from government by the Euromaidan street demonstrations that broke out in Kyiv in late 2013. Ukraine was voting a new leader to take his place. The Crimea portion of Ukraine had already been taken by Russia, and a separatist organization with Russian support was carrying out an armed uprising in the east. Additionally, the physical conflict was being waged online.[16]

4. Cyber Attacks on Government websites and Banks
   Assaults against websites belonging to the Ukrainian government in January 2022, One day after unsuccessful US-Russian talks on Ukraine's membership in NATO, the Russians launch attacks on government websites, and in February 2022, after Russian soldiers entered Ukraine's eastern regions, they take down a number of important governmental and financial websites. Russian assailants were blamed for the assaults by US intelligence, despite the Russian government's denials.[17]

Hybrid warfare is a strategy applied by Russia in annexing Crimea in the 2014 Ukraine conflict. In its application, the successful use of this strategy is a blow to the West about the challenges of using unconventional forces as weapons in carrying out war. The strategic environment in the contemporary era indeed forces actors to apply tactics that are considered the most effective in achieving their interests. Currently the world is entering the Fourth Generation War phase where the battlefield is not only carried out within defined boundaries but throughout cyberspace due to increasingly modern technological advances. These strategic environmental conditions ultimately support future conflicts to be multi-modal and multivariant. Thus, asymmetric power carries a significant role as one of the indicators applied by states in projecting their interests. their interests.

3.3 NATO cooperation with Ukraine in cyber security

The 30th Steering Committee meeting of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) was conducted. The 27 Sponsoring Nations in the CCDCOE Steering Committee unanimously approved Ukraine's participation as a Contributing Participant in the NATO CCDCOE. Ukraine's membership in the NATO CCDCOE as a Contributing Participant was put to a vote in the CCDCOE Steering Committee after a letter was delivered to reiterate its continued interest in doing so. The Center has already increased the number of its members from beyond the NATO countries.

The mapping activities to form a strategic vision is a difficult undertaking, complicated by the fact that many parties involved, both governmental and commercial, have chosen not to publicize their activities. However, enough information is publicly available to provide a basic conceptual framework with illustrative examples showing the scope of activities undertaken. Table 1 below shows the six lines of action, covering the types of tasks carried out and the opportunities used by public and commercial entities.

Table 1. The Activities of Governmental and Commercial actors to support the Ukraine Cyber Defense

No	Activities	Description	Taken by Government	Taken by Commercial
1	Network defence deployed	Cybersecurity personnel sent to Ukraine	U.S. Cyber Command "hunt forward" missions as tensions rose	-
2	Network defense remote	Cybersecurity operations	UK funding of private sector cybersecurity services	Vendors including Google, Microsoft, BitDefender, Cisco, Cloudflare, ESET, and Sophos providing free access security services for Ukrainian users
3	Threat intelligence	Sharing of classified and proprietary material	NATO states agencies sharing intelligence with Ukrainian partners	Vendors listed establishing mechanisms for rapid sharing of intelligence with Ukrainian partners
4	Capacity building	Coordination, Training, Policy, Building and Institution	Ukraine's admission to NATO's CCDCEO as a partner	Availability of Amazon Web Services cloud training to Ukrainians
5	Technical robustness	Provision of hardware and technical measures	Hardware upgrades provided by donor governments	SpaceX providing Starlink satellite communications units for civil and military use
6	Cloud enabled resilience and robustness	Migration of data and services to servers located outside Ukraine	-	Microsoft migrating government agencies enterprises free of charge

Source : Carnegie (9)

Ukrainian cybersecurity officials believe this international support was necessary to limit the effectiveness of Russian cyberattacks, the response and countermeasures were carried out on a much larger scale than Ukraine could have achieved on its own, enabling it to stop attacks that could have caused strategic casualties. The CCDCOE is a training and exercise facility, research institution, and centre for cyber expertise recognized by NATO. The multinational military organization with headquarters in Tallinn prioritizes multidisciplinary applied research as well as consulting, training, and exercises in the area of

cyber security [9].According to a statement from Ukraine's National Security and Defense Council, the collaboration would enable Ukraine and NATO to more successfully combat common cyberthreats, particularly those from Russia (NSDC). This collaboration is advantageous to both sides. Ukraine will get access to cutting-edge NATO research and technology, and CCDCOE members will learn more about how to protect against cyberattacks in times of conflict from Ukraine.

Beginning in the 1990s, NATO's relations with Ukraine have grown to become one of the alliance's most important alliances.

1. NUC has managed Ukraine's Euro-Atlantic integration process since 2009, including improvements made in accordance with the Annual National Program (ANP).
2. Ukraine actively participates in NATO-led operations and missions, deepening their mutually beneficial cooperation over time. Supporting comprehensive security and defense reforms, which are crucial for Ukraine's democratic growth and for boosting self-defense capabilities, is prioritized.
3. Since the July 2016 NATO summit in Warsaw, Poland, the Comprehensive Assistance Package (CAP) for Ukraine has formalized NATO's tangible assistance for Ukraine. The Ukrainian parliament enacted a bill in June 2017 designating NATO membership restoration as a priority foreign and security policy goal.
4. The related changes to the Ukrainian Constitution went into effect in 2019. President Volodymyr Zelenskyy gave his approval to Ukraine's new national security plan in September 2020, which calls for building a special relationship with NATO in order to join the alliance. [10]

Ukraine's cyber defenses have been improved via years of cooperation between NATO and Ukraine. The risky cyber activity of today has been discussed by NATO and Ukrainian cyber specialists in Brussels. Local Ukrainian authorities are also supported by foreign professionals who are present in the nation. A deal on bolstering cyber cooperation, including Ukraine's access to NATO's malware information sharing platform, will be signed soon between NATO and Ukraine. Ukraine will continue to receive resolute political and practical backing from NATO.

3.4 History of CCDCOE

The CCDCOE was established on May 14, 2008, during negotiations between Estonia and various countries, including Germany, Spain, Italy, Latvia, Lithuania, and the Slovak Republic. The Center was given full accreditation and international organization status for the same year by the North Atlantic Council in October. A symposium on the condition of the Maya world was sponsored by the CCDCOE in 2009, with an emphasis on studies on Mayan disputes as well as legal and technological challenges. The International Conference on Cyber Conflicts (CyCon), which adheres to the highest standards of academic writing, has helped to build a professional cyber security community during the course of its existence. The largest and most complete worldwide cyber training program in the world, Locked Shields, has been provided by CCDCOE since 2010. The aforementioned method has had a detrimental effect on CCDCOE members who are eminent international law professors from various nations as well as legal advisers from over 50 other countries and partners. The Second International Book of International Law's "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" was revised in 2017 and supersedes the initial release from 2013. This is achieved by completing a more extensive legal review against domestic legislation that considers each individual within the park's reach and international law, which restricts the use of force or armed conflict. . The Tallinn Manual 2.0 provides the most comprehensive examination of how international law now applies in cyberspace. For all NATO branches within the Alliance, the CCDCOE

has made a commitment to finding and coordinating education and training solutions from January 2018. The Transformation of the Supreme Allied Commander (SACT), one of the two NATO strategic command commands, has given CCDCOE the official title of "Head of Cyber Defense Operations Education and Training Department." In 2020, the CCDCOE will be established and grow to encompass 28 member countries, including NATO and Partners that share an Alliance boundary.

3.4.1 Mission & Vision CCDCOE

CCDCEO mission is to provide our NATO allies and member countries with specialized, interdisciplinary knowledge in cyber defense research, training, and exercises with a focus on technology, strategy, operations, and law. The goal is to encourage collaboration between like-minded countries. We bring together partners outside the Alliance as well as NATO Allies. CCDCOE are pleased to offer a interesting intrigue approach to the foremost significant issues in cyber defense with our inquire about, trainings and works out.

3.4.2 Meaning CCDCOE

The NATO "*Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defense expertise*" [11].

3.5 Strategy of CCDCEO to enhance Ukraine's cyber defense

Advances in information technology have gradationally changed the world. Cyberspace has come more extensive and open, adding freedoms and openings for people, perfecting society, creating a new interactive global online business for ideas, exploration and invention, promoting responsible and effective government and active citizen participation in state administration, working problems of original significance, icing government translucency and helping to help corruption. still, the advancement of the ultramodern digital world and the development of information technology have led to the emergence of new pitfalls to public and transnational security. In addition to incidents of natural origin, cyberattacks motivated by the interests of countries, groups, and individuals are adding in number and strength. There are adding cases of illegal collection, storehouse, use, destruction and dispersion of particular data, as well as illegal fiscal deals, theft and fraud on the Internet. The ongoing miliraty aggression by the Russia and other basic changes in Ukraine's external and internal security terrain bear the immediate establishment of a public cybersecurity system as an integral portion of Ukraine's public security. The purpose of the Cybersecurity Strategy of Ukraine is to produce conditions for the safe operation of cyberspace and cyber operations for the benefit of people, association and the nation.

3.6 CCDCOE Strategy for developing Ukraine's cyber security

CCDCEO's priority in improving Ukraine's cyber security is the development of such secure technologies and communications:

1. The development of a national security operations policy in the cyber sphere, aligning it with fairly advanced EU standards
2. Creating a work ethic on state and technology-based regulations, harmonizing regulations on communication, information protection, and privacy.
3. Creating a cooperative environment, and providing security services for every individual
4. Development of mobile communications such as, development of communication device cyber technology, Management of hardware security, content security, application systems, and communication service security

5. Organizations to draft cybersecurity concept papers
6. Enhancing citizens' digital skill and promoting a culture of safety and safe behavior in cyberspace, improving the knowledge, skills and abilities needed to achieve cybersecurity goals
7. Implementation of state and social projects to raise digital awareness of society in the area of cyber threats and cyber defense
8. Provide training on cyber emergencies and incidents
9. Enhancement of the national monitoring system of security status information and development of an integrated information security control system, implementation of global best practices and international standards in the field of cybersecurity and cyber defense.
10. Development of electronic communications infrastructure, including broadband internet access, digital and interactive television.
11. Develop a network of cyber incident response teams
12. Creation of a system for the timely detection, prevention and neutralization of cyber threats, including the involvement of voluntary organizations
13. Development and improvement of the technical and cryptographic information protection system
14. Strengthening international cooperation and supporting international initiatives in the field of cybersecurity served Ukraine's national interests
15. Deepening cooperation with the EU and NATO to strengthen Ukraine's cybersecurity capabilities16th 16. Participation in OSCE-led confidence-building activities in cyberspace
17. Create conditions for introduction of modern cyber defense technologies in Ukraine [12]

Appropriate conditions for engaging in cybersecurity activities in Ukraine should be created for certain companies, institutions and an association specializing in e-communications, information security, and owning operating critical infrastructure, regardless of their form of ownership. According to the law, matters of mandatory information protection and cyber defense measures are to be regulated and state authorities are to be supported in fulfilling their tasks in the area of information security and cyber defense. The state encourages the participation of research institutes, academic institutes, non governmental organizations, governmental organizations, and the individual in the development of cyber security and cyber defense countermeasures and implementation. As stated in Article 5 of the Washington Treaty, this treaty saves future generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind, and reaffirm faith in human rights, in the dignity and worth of the human person, in the equal rights of men and women and of nations great and small, and establish conditions in which justice and respect for obligations arising from treaties and sources of international law can be maintained, and promote social progress and better standards of living in greater freedom. [13]

4. Conclusion

NATO has played a very important role both to improving Ukraine's cyber security, and to preventing cyber attacks that are often carried out by The Russian , of course this is inseparable from the role of CCDCEO as one of NATO's developments in the field of cyber defense, in this conflict NATO has become an important pillar for Ukraine's vulnerable cyber defenses, Ukraine itself has made many technological changes since joining the CCDCEO, NATO takes this into account in establishing cooperation with Ukraine, NATO's motivations for supporting Ukraine are also inseparable from security interests of member states, such as easier surveillance of Russia, which is known to be one of NATO's biggest threats, by making Ukraine a member, NATO will also gain greater advantages and opportunities in competition with Russia. This is why NATO has taken the threat to cyberspace from state and non-state actors seriously

for so long, and has taken strict measures to protect itself from cyber attacks.skills and knowledge come from experience, and Ukraine certainly has valuable experience from previous cyber attacks, which adds significant value to NATO's CCDCOE. As the CCDCOE host country, Estonia is a long-term partner of Ukraine in building its cybersecurity and cyber-resilience capacities. Cooperation between the CCDCOE has increased tensions in this dispute. Russia's insistence on preventing Ukraine from joining NATO, describing membership as a threat to Russia's "historic future of the nation," appears to be the root cause of the current conflict, even though Ukraine has been associated with the organization for nearly three decades. It is also necessary to recognize that the operation results in eight months of warfare do not equate to permanent and comprehensive collective defense structures in cyberspace. The war has not solved the deep problems of sovereignty, accountability and burden-sharing. Yet among those who participate in and sponsor advocacy, there is a palpable sense that something important is happening; Several partners strive for common values and challenge the previous assumptions of , which the cybercriminal will always defeat.

References

[1] Samad, Yusuf. *Understanding The Russian Cyber Warfare and The Role of The State Intelegency Agency in Countering Cyber Threats* (2022). Vol 24. No 2. 2022. 18-26

[2] Priyono, Ujang .*Cyber Warfare as a part of Russia-Ukraine War*, Vol 8, no 2. 2022. 12-13

[3] Made, Aryawan, *The Role of UN as an International in The Conflict of Russian*-Ukraine. 2023, Vol 4. No 1 14-25

[4] Rohman, Sayful. *Russia-NATO Rivalry and Strategic Influence in Eastern Europe on Security and Economy.* POLITICON: Journal of Political Science Vol.3, No.1. 2021. 111-132

[5] Rum, Azhar. *Practical Use of Cyber Operation (CYBER WARFARE) In Conflict Armed Conflict from the Perspective of International Humanitarian Law.* DEPARTMENT OF INTERNATIONAL LAW FACULTY OF LAW HASANUDDIN UNIVERSITY MAKASSAR. 2021

[6] Bystrova, Bogdana.*Comparative Analysis of Curricula for Bachelor's Degree in Cyber Security in the USA and Ukraine*. Comparative professional pedagogy 7.4 (2017): 114-119.

[7] Spinu, Natalia. *Ukraine Cyber Security*. Article of DCAF Geneva Headquarters. 2020 https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGoernanceAssessment.pdf

[8] Baezner, Marie. (2018). Cyber and Information warfare in the Ukrainian conflict. Zurich, ETH Zürich. 35

[9] Beckroff, Nick . *Evaluating the International Support to Ukrainian Cyber Defense*. *Carnegie article of Ukraine Cyber Defence* (2022). https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian--defense-pub-88322

[10] Wolff , Andrew. *The future of NATO enlargement after the Ukraine crisis* (2015). Vol 91. No 5. Oxford University Press

[11] "About us". 2023. Ccdcoe.Org. https://ccdcoe.org/about-us/.

[12] *CYBER SECURITY SRTATEGY OF UKRAINE. A provision Approved by Presidential of Ukraine No. 96/2016 dated 15 March 2016.* https://ccdcoe.org/uploads/2018/10/NationalCyberSecurityStrategy_Ukraine.pdf

[13] *A comparative analysis of Article 5 Washington Treaty* (NATO) and Article 42(7) TEU(EU)https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/739250/EPRS_ATA(2022) 739250_EN.pdf

[14] Brian, Prince. *'Operation Armageddon' Cyber Espionage Campaign Aimed at Ukraine: Lookingglass*. CybersecurityNetwork. 2015.https://www.securityweek.com/operation-armageddon-cyber-espionage-campaign-aimed- ukraine-lookingglass/

[15] Sanger, David. Suspicion Falls on Russia as 'Snake' Cyberattacks Target Ukraine's Government. New York Times. 2014https://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake- cyberattacks-target-ukraines-government.html

[16] Zemlianichenko, Alexander. Election Cyberattacks: Pro-Russia Hackers Have Been Accused in Past. NBC News. 2016. https://www.nbcnews.com/mach/technology/election-cyberattacks-pro-russia-hackers- have-been-accused-past-n673246

[17] Harding, Luke. Ukraine hit by 'massive' cyber-attack on government websites. The Guardian. 2022.https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers