International Journal of Multidiscipline

TLEP – International Journal of Multidiscipline
(Technology, Language, Education, and Psychology)
ISSN: 2488-9342 (Print) | 2488-9334 (Online)

Open Access | Peer-Reviewed | Monthly Publication | Impact factor: 8.497 / 2025

The Role Of International Organizations In Ensuring Cybersecurity (UU, Interpol, Enisa And Others)

Rasulova Shahzoda,
computer science teacher at Academic Lyceum
No. 1 under the Ministry of Internal Affairs of the Republic of Uzbekistan

Abstract
This article examines the growing importance of international organizations in combating cybersecurity threats in a globalized world. As threats transcend national borders, the need for a cooperative response is also increasing. The article analyzes the roles and actions of the United Nations (UN), the International Criminal Police Organization (INTERPOL), the European Union Agency for Cybersecurity (ENISA), and other key organizations. The efforts of these organizations in terms of standard-setting, capacity-building, intelligence sharing, and legal instruments are discussed, as well as the challenges they face. The study concludes that cooperation between these agencies is crucial for ensuring stability, trust, and resilience in cyberspace.
Keywords: Cybersecurity, international cooperation, UN, INTERPOL, ENISA, cybercrime, cyber truce, data sharing.

Introduction

The 21st century world of technology has rapidly transformed all aspects of society, but along with these benefits, it has also brought new and complex threats in cyberspace. Cybercrime, data breaches, and attacks on national infrastructures are no longer local or regional problems, but global in nature. No single state, even the most developed one, with all its resources, can address these multifaceted threats alone [1]. It is to address this challenge that international organizations have emerged as important mediators and catalysts in the field of cybersecurity.

The aim of this article is to examine in depth the role of the UN, Interpol, ENISA, and other key international forums in shaping cybersecurity and fostering global cooperation. The article analyzes the various roles of these organizations, including policy development, legal frameworks, technical capacity building, and law enforcement cooperation. It also highlights the obstacles they face, such as sovereignty, technological asymmetry, and political opposition.

Analysis and Discussion

The United Nations (UN): Normative Framework and Shaping International Law

The UN is at the heart of the global cybersecurity debate due to its unique international mandate. The UN's role is primarily focused on maintaining international peace and security, and this mandate now extends to "cyberspace." [2] The UN's work in this area is carried out through a number of instruments and organizations.

The State Group on Information and Telecommunications (SGT), established by the General Assembly, is the main platform for discussions on confidence-building measures and the application of international law in cyberspace. Several SGT reports have developed a number of important principles for the conduct of States in cyberspace, such as respect for State sovereignty, the protection of human rights, and the application of the laws of modern warfare. [3] In recent years, the UN has also established an Open Working Group (OEWG), which, since the GGE is composed of only a limited number of

members, facilitates more inclusive discussions [4].

Other UN bodies, such as the Office of Counter-Terrorism (UNOCT), combat the use of digital means to finance terrorism, and the Human Rights Council works to protect the right to privacy in cyberspace. The UN's role is thus largely to lay the foundation for a global cybersecurity architecture, both normatively and legally.

Interpol: Law Enforcement Cooperation and Operational Capability

While the UN focuses on the political and diplomatic aspects of cybersecurity, Interpol focuses directly on the practical and operational aspects of combating cybercrime. Interpol's global network of police departments makes it particularly effective in combating crime [5].

Interpol's Cybercrime Unit works to enhance law enforcement capabilities, support criminal investigations, and facilitate international arrest requests. The organization regularly conducts "Operation Days," conducting simultaneous cybercrime raids in multiple countries, which have resulted in the arrest of hundreds of suspects and the blocking of hundreds of websites. [6] In addition, Interpol has helped strengthen local capabilities by establishing specialized cyber investigation units (Digital Forensics Labs) in more than 50 countries around the world.

Interpol's most important contribution is its international information exchange platform (I-24/7), which provides real-time access to criminal databases in member states, including information on fraud or malicious software features. This type of operational cooperation is essential in combating cybercriminals operating across borders.

European Union Agency for Cybersecurity (ENISA): Regional Cooperation and Standardization

Established by the Council of the European Union in 2004, ENISA is a strong example of regional integration in the field of cybersecurity. Its role is to support a high, uniform level of cybersecurity in the European Union [7].

ENISA mainly operates in three areas:

1. Providing technical assistance in the implementation of European legislation, such as the SIEM (NIS) Directive. The Agency helps EU Member States develop national cybersecurity strategies and develops technical standards for critical infrastructure operators [8].
2. Capacity building and training. Through programmes such as Cyber Europe, ENISA organises exercises and training between EU countries in response to cyber incidents, testing and strengthening their collective response capabilities.
3. Promoting research and innovation. The agency conducts in-depth research on emerging threats, such as Artificial Intelligence and IoT security, and promotes cooperation between industry and academia across Europe.

ENISA plays a key role in developing a cybersecurity certification framework for the European Union, which sets common standards for products, services and processes and increases trust and mutual recognition in the European market.

Other Key Organisations: NATO, OECD and Regional Organisations

- North Atlantic Treaty Organisation (NATO): NATO focuses on strengthening cyberspace in line with its collective defence mandate. In 2016, cyberspace was officially recognised as a NATO battlefield [9]. NATO has a Cybersecurity Centre to enhance the ability of member states to withstand cyberattacks, as well as to facilitate political dialogue on "cyber disarmament" initiatives.
- Organisation for Economic Co-operation and Development (OECD): The OECD approaches cybersecurity from an economic and development perspective. It has established the basis for considering data privacy, personal data protection and security as important factors for economic

growth through documents such as the 1980 Privacy Directive and the 2002 Information Systems and Networks Security Directive [10].

• Regional Organizations (ASEAN, OAS, African Union): Regional organizations such as the African Union (African Union Convention on Cyber Security) and the Organization of American States (OAS) play an important role in developing cybersecurity policies and legal frameworks that are appropriate to their cultural, economic and legal contexts. They serve as platforms for developing local capabilities and fostering regional cooperation.

Other Important Organizations: NATO, OECD and Regional Organizations

North Atlantic Treaty Organization (NATO): NATO focuses on strengthening cyberspace in line with its collective defence mandate. In 2016, cyberspace was officially recognized as a NATO battlefield. NATO has a Cybersecurity Center to enhance the ability of member states to withstand cyberattacks, as well as to conduct political discussions on “cyber disarmament” initiatives. Organization for Economic Co-operation and Development (OECD): The OECD approaches cybersecurity from an economic and development perspective. It has established the basis for considering data privacy, personal data protection, and security as an important factor for economic growth through documents such as the 1980 “Privacy Directive” and the 2002 “Guideline on the Security of Information Systems and Networks”. Regional Organizations (ASEAN, OAS, African Union): Regional organizations such as the African Union (African Union Convention on Cyber Security) and the Organization of American States (OAS) play an important role in developing cybersecurity policies and legal frameworks that are appropriate to their cultural, economic, and legal contexts. They serve as a platform for developing local capabilities and fostering regional cooperation.

The Importance of the Topic in Education

International cooperation in ensuring cybersecurity is strengthened not only by political and operational actions, but also by deep integration into the educational sphere. In today's digital world, cybersecurity literacy has become not only the task of elite specialists, but also a necessary life skill for every citizen. Therefore, it is of strategic importance to instill this topic at all levels of education. Teaching students at the primary and secondary levels the basics of digital hygiene, namely, creating strong passwords, identifying phishing attacks, protecting personal data, and the rules for safe behavior on social networks, will lay the first brick of the "human defense wall" in society. This will allow the younger generation to be educated not only as potential victims, but also as conscious digital citizens. And the issue becomes even more serious in the higher education system. The demand for qualified cybersecurity professionals worldwide is far higher than the supply, creating a “skills gap”. International organizations play an important role in this regard. For example, ENISA helps to harmonize professional education by developing EU-wide cybersecurity competency standards and organizing training courses such as “Cyber Europe”. This approach ensures that professionals trained in different countries work effectively with each other. Interpol’s establishment of specialized cyber search laboratories around the world and the training of law enforcement officers is a vivid example of practical and specialized education. It includes not only technical knowledge, but also the legal and procedural aspects of investigating cybercrime. Normative documents and principles developed by the UN and OECD

serve as the foundation for creating curricula in universities for subjects such as cyber law, digital ethics and international cyber policy. They teach students not only how to protect systems, but also why and based on what legal and ethical standards they should be protected. Thus, international cooperation in education is the most sustainable and proactive approach to combating future threats, which not only creates a pool of qualified personnel, but also increases the resilience of society as a whole to the dangers in cyberspace.

Relevance of the Topic

The role of international organizations in ensuring cybersecurity has never been more relevant than it is today. This is because threats in cyberspace are growing dramatically in scale, complexity and impact. First, cybercrime has become a huge economic burden. Ransomware attacks, data theft and financial fraud cause trillions of dollars in damage to the global economy every year. This directly affects not only large corporations, but also small businesses and ordinary citizens. It is no coincidence that structures such as the Organization for Economic Cooperation and Development (OECD) consider cybersecurity an indispensable condition for sustainable economic growth. Second, cyberspace has become a new arena of geopolitical confrontation. NATO's recognition of cyberspace as a full-fledged battlefield, like land, sea and air, means that conflicts between states have moved to the digital world. State-sponsored hacking groups are increasingly using cyberattacks to spy, disrupt critical infrastructure (power plants, water systems, healthcare facilities), and interfere in the internal affairs of other countries through disinformation campaigns. This poses a direct threat to the national security of any country and makes the efforts of organizations such as the UN to maintain international peace more important than ever. Third, the rapid development of technology is creating new and unpredictable risks. Artificial intelligence (AI) can create autonomous and self-adaptive malware, and quantum computing technologies have the potential to defeat almost all current encryption standards. In the face of such fundamental changes, it is vital that the international community jointly develop new standards, protocols, and trust measures. Fourth, the interconnectedness of the modern digital economy creates a chain reaction of threats. A single attack on the software supply chain can simultaneously affect thousands of organizations. This clearly shows that no single country can protect itself in isolation. Therefore, the work of Interpol's data exchange platform and ENISA on regional standardization is of particular importance. In conclusion, the relevance of this topic is that cybersecurity is no longer just the work of IT specialists, but also of economic stability,

Challenges and Future Directions

While international organizations do important work, they face serious obstacles. These include concerns about state sovereignty, geopolitical confrontations between major powers such as the United States, Russia, and China, the digital divide between developed and developing countries, and the rapid development of cyberweaponization [11]. In addition, the intersection of mandates and interests of different organizations can sometimes lead to duplication of work and an uneven distribution of resources.

In order to improve the effectiveness of these organizations in the future, it is necessary to strengthen cooperation between them, increase the number of staff of member states and expand technical capacity-building programs. It will also be important to develop new international agreements and protocols aimed at responding to threats arising from new

technologies such as artificial intelligence and quantum computing.

Conclusion

In conclusion, the UN, Interpol, ENISA and other international organizations are integral parts of the global cybersecurity landscape. They play different but complementary roles: the UN sets international law and norms, Interpol facilitates practical criminal investigations and arrests, and ENISA focuses on regional standardization and capacity-building. Without their collective efforts, the chaos in cyberspace would only increase. As the digital transformation continues, the importance of these organizations will increase. Their continued development, innovation, and, most importantly, collaboration will be key to ensuring a safe, secure, and reliable environment for the globalized digital economy.

REFERENCES

Dunn Cavelty, M. (2013). Kiberxavfsizlik va kiberxavf: Milliy xavfsizlikka nisbatan yondashuvlarni tahlil qilish. Routledge. 25-47-betlar.

United Nations. (2021). Kiberfazoda xalqaro tinchlik va xavfsizlikni ta'minlash bo'yicha yakuniy hisobot. Bosh Assambleya Rasmiy hujjatlari, 75/240. 5-bet.

United Nations Group of Governmental Experts (UNGGE). (2015). Kiberfazoda ishonchni oshirish choralari va xalqaro huquqning qo'llanilishi bo'yicha yakuniy hisobot. 13-bet.

United Nations Open-ended Working Group (OEWG). (2021). Kiberfazoda xalqaro tinchlik va xavfsizlik bo'yicha yakuniy hisobot. 3-bet.

Interpol. (2020). *Interpol Global Kiberfazo Strategiyasi 2020-2023*. 7-bet.

Interpol. (2022). Interpol Yillik Hisoboti 2022. "Kiberjinoyat" bo'limi, 21-bet.

European Union Agency for Cybersecurity (ENISA). (2022). ENISA mandati. https://www.enisa.europa.eu/about-enisa (17.10.2023 da olindi).

Christou, G. (2016). Yevropa Ittifoqida kiberxavfsizlik: Globallashgan axborot jamiyatini o'rganish. Palgrave Macmillan. 89-112-betlar.

NATO. (2016). Varshava Sammiti Kommunikesi. 72-band.

Organisation for Economic Co-operation and Development (OECD). (2002). Axborot Tizimlari va Tarmoqlari Xavfsizligi Ko'rsatmasi. 9-bet.

Nye, J. S. (2017). Kiberfazodagi kuch: Deterrens va diplomatiya. "Foreign Affairs" jurnali, 96(3), 10-15-betlar.

Tikk, E., & Kerttunen, M. (2020). BMT kiberfazo davlati guruhlari bo'yicha qo'llanma. Ginevada xavfsizlik siyosati markazi. 45-67-betlar.

Maurer, T. (2018). Kibermeros: Kiberdavlatlar xalqaro hamkorlikni qanday shakllantiradi. Harvard University Press. 102-125-betlar.

Carr, M. (2016). Kiberxavfsizlikning siyosiy iqtisodi: Davlatlar, chegaralar va internet. "Review of International Studies" jurnali, 42(3), 459-482. 470-bet.

Shackelford, S. J. (2020). *Kiberfazoda tinchlikni qurish: Kibertinchlikni qanday shakllantirish mumkin*. Oxford University Press. 178-201-betlar.