academic publishers
INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE (ISSN: 2692-5206)
Volume 04, Issue 09, 2024
Published Date: 03-11-2024

REGULATION OF COOPERATION BETWEEN STATE AND NON-STATE ENTITIES IN THE FIELD OF CYBER SECURITY

Mirzakhakimova Shodiyabegim Mirzohid qizi
Tashkent State Law University
4th year student of the Faculty of international law and Comparative Law

Abstract: This article explores the collaboration between state and non-state entities in the field of cybersecurity, focusing on the regulatory frameworks that underpin these partnerships. As cyber threats become increasingly sophisticated and pervasive, effective cooperation between governments, private sector organizations, and non-governmental entities is essential for enhancing overall cybersecurity resilience. The paper examines key examples of successful collaborations, such as partnerships between national cybersecurity agencies and private companies, as well as international initiatives that foster information sharing and best practices. It also addresses the challenges and obstacles faced in establishing effective cooperation, including regulatory discrepancies, trust issues, and the dynamic nature of cyber threats. By highlighting the importance of structured collaboration and proposing potential regulatory solutions, this article aims to contribute to the ongoing dialogue on improving cybersecurity strategies and frameworks globally.

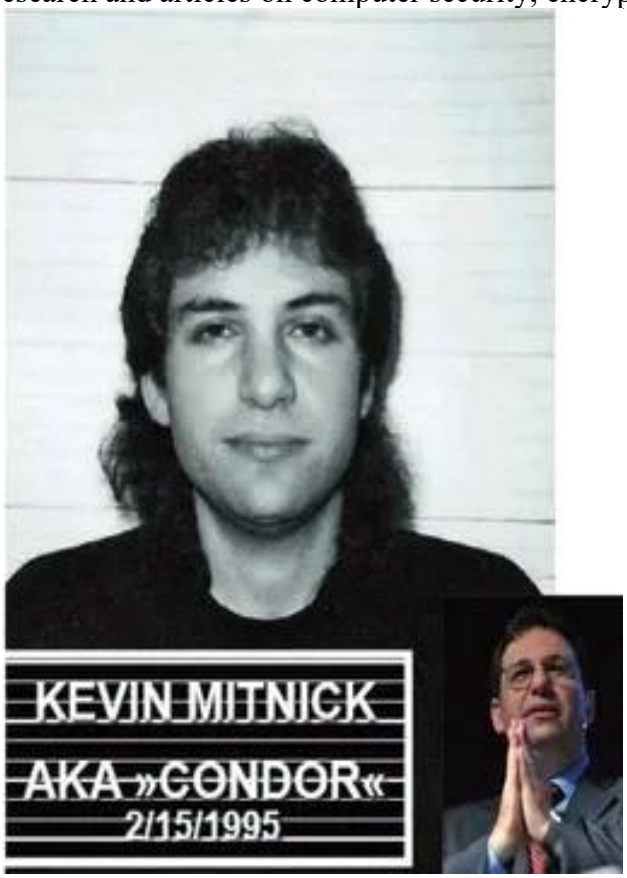
Introduction

Cybersecurity stands out as a global problem in the modern world. Along with the widespread use of digital technology and the internet, cyber threats are also becoming more and more intense. Cooperation between state and non-state entities is one of the effective solutions to counter cyber threats. The technological innovations and experiences that exist in the private sector, together with government bodies, help to improve cyber security. At the same time, states play an important role in the regulation and control of cyber security, which supports the activities of the private sector and sets safety standards.This article covers the issues of regulating cooperation between state and non-state entities. The article analyzes successful collaborations in the field of cybersecurity, their regulation and the problems that arise. It also offers the approaches and strategies needed to effectively organize cooperation. Strengthening cooperation in the cybersecurity process is important not only in eliminating threats, but also in increasing global security.

Discussion and results

Cybersecurity (cybersecurity) is the process of protecting information systems, organizations, networks and data from cyber threats. The main purpose of cyber security is to protect data, systems and infrastructure by ensuring security, privacy and integrity.The following scientists have conducted research in the field of cyber security.

Bruce Schneider is a leading information security expert. He sees cybersecurity as a global problem and emphasizes the balance of technology and human factors to ensure security. Bruce Schneider is a famous American security expert, writer and expert in the field of technological security. He is primarily known for his research and articles on computer security, encryption, and information security.



Kevin Mitnick: Kevin Mitnick is a famous American computer security expert and former hacker. He was born on August 6, 1963, and became known in the 1990s for his illegal access to many computer systems.

Mitnick has employed a variety of techniques since the 1980s to gain access to large companies and organizations, including businesses such as IBM, Nokia, and Motorola. He was known for his social engineering abilities, through which he deceived people and obtained the necessary information from them.In 1995, he was arrested by the federal government and sentenced to 5 years in prison for Computer Crimes. He was released in 2000. After his release, Mitnick began working as a computer security consultant. He dedicated his knowledge and expertise to enhancing security and applying it to organizations in defense. He is the author of books such as" the Art of Deception"," The Art of Intrusion", and" Ghost in the Wires". In these works he presents his experiences in hacking activities, social engineering and security.

Uzbekistan has a number of laws and regulatory documents aimed at ensuring and protecting cybersecurity. They include the following basic laws:
1.”Cybersecurity Act of the Republic of Uzbekistan".
This law, adopted in 2021, sets the basic standards for ensuring cybersecurity, combating cyber attacks and threats, as well as increasing the security of Information Systems.
2. "Informatization act".
The Act, passed in 2002, sets out provisions for the protection of information resources and the use of Information Technology.
3. "State secret Protection Act".
Law aimed at protecting state secrets and ensuring their safety. This law is important in the context of cybersecurity.
4. "E-Government Act".
Law dedicated to the introduction of electronic public services and information and communication technologies. It includes provisions aimed at ensuring the safety of electronic services.
6.Decrees and resolutions of the president of the Republic of Uzbekistan - there are a number of decrees and resolutions that determine public policy in the field of cybersecurity. They are aimed at ensuring cybersecurity, training and improving staff skills.
7. Regulatory acts of the Ministry of Economy and industry of the Republic of Uzbekistan and other state bodies-various regulatory acts and regulations governing cyber security practices.

A number of non-governmental organizations operate in the field of cyber security in Uzbekistan and play an important role in the development of international cooperation. Below is information about such organizations and their cooperation with other countries:
1. It Association of Uzbekistan
It Association of Uzbekistan brings together entrepreneurs and organizations in the field of Information Technology. It develops and practices strategies to ensure cybersecurity.The association cooperates with international IT organizations, including the UN and other regional organizations. As part of these collaborations, there are opportunities to learn and adopt best practices in the IT field.
2. Cyber Security Center Of Uzbekistan.
This center conducts events aimed at identifying and eliminating threats in the field of cybersecurity. The center also collects and analyzes information about cyberattacks and threats.The center interacts with international cyber security organizations, in particular with the European Union and the UN. These collaborations help develop and comply with global cyber security standards.
3. Ministry of education and innovation of Uzbekistan
The Ministry of education and innovation carries out programs aimed at improving knowledge and training of young people in the field of cyber security.The ministry cooperates with international educational organizations, including UNESCO and other UN agencies. These collaborations help promote cybersecurity education and share experiences.
4. Internet Association Of Uzbekistan
This non-governmental organization holds events aimed at ensuring internet security and protecting users from cyber attacks.The Internet Association of Uzbekistan cooperates with regional and international organizations, in particular, with international organizations for internet management. These collaborations aim to increase internet security and protect users.

5.Non-governmental cyber security organizations
A number of non-governmental cyber security organizations, such as Cyber Security Uzbekistan, hold cyber security workshops and trainings.Such organizations are aimed at developing international cooperation with the aim of exchanging mutual experience from the international cyber security event and combating cyber attacks.

Non-governmental organizations operating in the field of cyber security in Uzbekistan play an important role in the development of international cooperation. They help to carry out programs aimed at exchanging experience with other countries, operating in accordance with global standards and ensuring cybersecurity. This leads to improved cybersecurity in Uzbekistan.Uzinfocom and ZiyoNet are important organizations operating in the field of cyber security and Information Technology in Uzbekistan. Their international partners are as follows:
1. UN (United Nations)-assists in the implementation of development projects in the field of Education, Information and Communication Technology.
2. The European Union cooperates by providing expertise and resources on Information Technology and cyber security.
3. The Asian Development Bank (ADB) provides financial and technical support for Information Technology and infrastructure development.
4. World Bank-supports investment and development projects in the field of Education and cyber security.
5. UNESCO (United Nations Educational, Scientific and Cultural Organization) is a collaborative effort to promote innovation and Information Technology in education.
6. ITU (International Telecommunication Union)-assists in setting and cooperating standards in the field of Telecommunications and Information Technology.
7. OECD (Organization for Economic Cooperation and development)-assists in the development of recommendations and strategies for the use of Information and communication technologies.
8. Cybersecurity and Infrastructure Security Agency (CISA) is a U.S. – based cybersecurity and infrastructure security sharing and collaboration.
9.Cisco is a collaboration on network equipment and cybersecurity solutions.
10.Microsoft-projects on cloud technologies and digital transformation.
11.Huawei: - cooperation on the development of telecommunications infrastructure and cybersecurity.

Uzbekistan cooperates with a number of foreign countries in the field of cybersecurity. These collaborations aim to increase cybersecurity, share experiences and operate in accordance with international standards. Below are examples of Uzbekistan's cooperation in cyber security:
1.There are a number of agreements between Uzbekistan and Russia on cooperation in the field of cybersecurity. This cooperation is aimed at combating cyberattacks and protecting information systems.

2. There is cooperation between Uzbekistan and Kazakhstan for the exchange of experience in cyber security and the implementation of joint projects. Both nations are involved in programs aimed at ensuring regional security.

3.Uzbekistan and China are interested in developing cooperation in the field of cyber security. There are programs to share technological experience with China and prevent cyber attacks.

4. Cooperation between Uzbekistan and the United States in the field of cybersecurity is carried out, as well as by conducting mutual trainings and seminars. Uzbekistan is interested in using the experience of the United States in the field of cyber security.

5. Uzbekistan is trying to develop cooperation with the European Union in the field of cyber security. Within this framework, projects are being implemented to ensure cybersecurity and Exchange technological knowledge.

6. Uzbekistan cooperates with the UN and other international organizations in the field of cybersecurity. In particular, he is actively involved in UN cybersecurity programs.

7. Uzbekistan is participating in programs aimed at strengthening economic cooperation between regional organizations of Central Asia, including the SCO (Shanghai Cooperation Organization) and Uzbekistan.

Internationally, there are a number of important collaborations and initiatives in the field of cyber security. These collaborations are carried out between states, International Organizations, Non-Governmental Organizations and industry representatives to combat cyberattacks, threats and risks.
The following international organizations are active in cybersecurity.
1.There are a number of important examples within the framework of NATO(North Atlantic Treaty Organization)- cyber operations. Examples are given below:
a).NATO conducts major military exercises, such as the Cyber Coalition, in an effort to strengthen its cyber protection capabilities. As part of these exercises, member states practice together to counter cyber threats, detect and respond to attacks.
b).NATO provided assistance to member states during the WannaCry cyber attack in 2017. This cyber attack affected many organizations globally, and NATO offered technical assistance to its members to reduce the impact of the attack.
c).NATO has developed a rapid information sharing system about cyber threats and attacks. For example, in 2020, rapid response operations were carried out to exchange information about cyber threats between member states.
d).NATO provided cyber protection advice and support to Ukraine during Russia's cyber attacks on Ukraine in 2022. This support included the necessary technologies to detect and eliminate cyber attacks.
e).NATO is implementing various programs to enhance cyber security capabilities in its member states. For example, in 2021, research and training was conducted to combat cyber threats as part of the" NATO Cyber Defence Centre of Excellence".
These examples show how NATO cyber operations operate to counter a wide range of and contemporary threats.
3. Europol and INTERPOL
With the support of the European Cybercrime Centre(EC3), the European Union implemented a strategy to combat cyberattacks. EC3 assists in the collection and analysis of cybercrime information among member states.
INTERPOL implemented a global strategy against cybercrime Direction. It helps member states fight cybercrime and provides access to information on a global scale.
INTERPOL conducts international operations against cybercrime. For example, through operas such as" Operation Haechi", efforts are taken to identify and apprehend other criminals.
5. The Shanghai Cooperation Organization (SCO) has practically increased programs aimed at promoting regional cooperation in ensuring cybersecurity.A platform for implementation and security in cyber security will be created between the Tashkent nobles.
6.ICANN (international cybersecurity organization) to increase the practice of a killer new research and initiatives in the field of cybersecurity. These studies are important for enhancing internet Security and combating cyber threats.ICANN conducts research on cyber threats on the internet, such as phishing, DDoS documentation, and interesting applications. These studies have studied how threats spread and their taste for internet infrastructure.
7.Annual cybersecurity conferences and forums (e.g. rsa Conference, black hat) provide implementation opportunities among global experts and organizations.
Countries that resort to the best cooperation in the field of cybersecurity in the world are actively developing mutual implementation, resource use and cybersecurity strategies in the face of cyber attacks and threats. These states serve to improve their relations independently of global cybersecurity.
Cyber security is considered to be an important defense concern for past, high-risk countries. Unicorn mamalakats are at the forefront of cyber security level, trade, national strategies, and critical infrastructure protection. The fact that they have qualified specialists in this area undoubtedly contributed to their

development.Fraud prevention software company Seon derives from the global cyber strategies index and recent cybercrime Statistics data to determine which states have been deficient in the field . According to the cybersecurity ranking by country, the three safest states by bul rankings are:

Denmark. Denmark was 8.91 balls as the world's number one safe nation.

Germany. With wide coverage Games and questions, the German Seon ranking was 8.76 balls.

United States. Additional states have strong legislation and showed little information compared to cybercrime, which added them third place and 8.72 points.

The Australian Seon placed eighth on the list-a target achievement. However, recent problems in our yard have shown the need to improve cyber security strategies. This, most importantly, showed a passion for strategy and skillful power to implement them. Programs such as the master of online cybersecurity at unsv have helped meet this requirement. The suitability of online education with world-leading education is built on by developers building against global cyber problems and achieving success in a ever-changing industry with the support they need.

These international documents and books provide information about cooperation in the field of cyber security:

1)developing activities: the garden with cybersecurity is published by the State-Security Council, which carries out public-private partnerships and cooperation in the country, and the Organization of cooperation in Europe, Vienna, March 2023

2) cyberspace, non-state actors and the obligation to prevent cross-border damage-white rose research online (States are allowed to use their cyberinfraternity in a way that harms other states ' rights to international law. This obligation imposed a bilateral obligation on the states. The first duty was to prevent and punish valuable cyber behavior from the state arising from its territory, which gave local states the necessary places and support for the institution a wide margin of gratitude in deciding the design and content of this document. such. The second duty is when information comes from their cyberinfraternity and states have information about this information (real or construction), which means that they must use their capabilities and resources to manage it. What would be reasonable in the situation would be the garden to the factors of the type of activity being taken at that time, such as the resources available to the state and the risks of the garden with a particular activist. Together, these activities offer states to protect information from costly cross-border cyber behavior, which is simply provided by non-governmental organizations in international law creates a commitment. However, the structure of a garden international treaty or several international treaties with special cyberattacks is crucial to achieving safe cyberspace.)

3) Regulation (EU, Euratom) 2023/2841 European Parliament and Council 13 December 2023.

4) cybersecurity, Internet management, and the ambiguous direction: the role of non-governmental actors in the development of Internet Policy-

(Wolfgang Kleinwachter / honorary professor at Aarhus University: Commissioner, Global Commission on peace in cyberspace (GCSC))

5."Cybersecurity for leaders: A Practical Guide" - Isabella Kaminska, 2019.

6."Cybersecurity Essentials" - Charles J. Brooks, Christopher Grows Up, Philip Craig, 2017.

7."Public-private partnership in cyber security: a guide to state and local governments" is a cyber security and Infrastructure Security Agency.

8."Building a culture of cybersecurity: a guide to public-private partnerships" - John D. Suini, 2020.

9.The OSCE has defined cooperation in international sources:

"The problem of OSCE and cybersecurity" - V. V. Ponomarev, 2021.

"Cybersecurity and OSCE: a Global perspective" - various authors, 2022.

10."Cybersecurity: a beginner's guide" - Kevin Beaver, 2021.

11."Cybersecurity: An Introduction" - John McCumber, 2019.

Conclusion

Cybercrime and threats, including phishing, DDoS attacks and data corruption, are growing rapidly globally. This creates new risks for states and organizations. Modern technologies, such as artificial intelligence and machine learning, play an important role in providing cyber security. However, these technologies need to be applied correctly and efficiently. Cyber security issues are global in nature. Therefore, it is important to

strengthen the exchange of information and cooperation between states, effective cooperation between the public and private sectors is necessary in ensuring cyber security. This helps to share experiences in identifying and countering cyber threats.Cyber security training and training are important, as well as increasing cyber awareness among citizens and staff. Developing knowledge and skills in cyber security can help prevent cyber threats.

Suggestions

There are a number of initiatives and strategies to enhance international cooperation. Both in the field of cybersecurity and in the field of cyber security, these initiatives are aimed at ensuring effective cooperation between states, international organizations and the private sector. Below I bring some important suggestions:

1.Development and implementation of global policies to combat cybercrime with international organizations,i.e. the UN and UNODC. As well as conducting international operations in the detection and Prevention of cybercrime with INTERPOL and Europol.
2.Creating instant information sharing platforms about cyber threats and attacks: the introduction of systems for the rapid exchange of information about cyber threats between countries.
3.To develop joint cyber security strategies through regional organizations such as the European Union and NATO.
4.Training qualified professionals by conducting international cyber security trainings and workshops.Cyber security certification programs: training professionals through mutually recognisable certifications.
5. Providing cyber security and sharing experiences through partnerships with private companies.
6.International research and project development to enhance cyber security through new technologies such as artificial intelligence and blockchain.
7.To discuss cyber security policies between countries and organize international conferences and forums to reach agreements.
8.Global Cybersecurity Index (GCI): creating indexes to assess and compare countries ' cyber security levels.

References:

1. Kaspersky Lab. (2022). Cybersecurity Trends 2022: New Challenges and Solutions.
2. NIST. (2020). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.
3. ICANN. (2021). ICANN’s Role in Cybersecurity: Protecting the Internet’s DNS.
4. Europol. (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021.
5. INTERPOL. (2020). Cybercrime Strategy 2020-2025.
6. Shanghay Cooperation Organization.(2021).SCO Cybersecurity Cooperation: A New Approach.
7. Chen, T., & Zhao, J. (2020). Cybersecurity: A Comprehensive Guide. Springer.
8. Bertino, E., & Islam, N. (2017). "Botnets and Cybersecurity." Computer Security, 75, 115-128.
9. Symantec. (2022). Internet Security Threat Report. Symantec.
10. United Nations Office on Drugs and Crime (UNODC). (2021). Cybercrime Toolkit for Legislators.
11. 11.Shanghay Cooperation Organization.(2021). SCO Cybersecurity Cooperation: A New Approach.
12. 12. "EU Cybersecurity Strategy for the Digital Decade" (2020)
13. 13.United Nations Office on Drugs and Crime (UNODC). (2021). Cybercrime Toolkit for Legislators.
14. 14. https://www.gazeta.uz/oz/2024/06/26/iiv/
15. 15. https://www.lex.uz/uz/docs/-5960604
16. 16.https://csec.uz/uz/news/yangiliklar/xavfsizlik-sohasida-o-zbekiston-va-qozog-iston-respublikalari-o-rtasidagi-hamkorlikni-rivojlantirish/
17. 17. https://www.nato.int/
18. 18. "Council of Europe Convention on Cybercrime" (Budapest Convention) — 2001
19. 19. "General Data Protection Regulation" (GDPR)-2018.