ISRG Journal of Engineering and Technology (ISRGJET)

ISRG PUBLISHERS

Abbreviated Key Title: ISRG J Eng Technol.

ISSN: 3107-5894 (Online)

Journal homepage: https://isrgpublishers.com/isrgjet/

Volume – II Issue -I (January - February) 2026

Frequency: Bimonthly

From the perspective of international law, artificial intelligence and cyberwarfare (the legal position of state responsibility)

Prof. Dr. Erdal DURSUN[1*], Muaiyid Rasooli[2], Jamshid Rasooli[3]

[1] Rector, International Science and Technology University, Warsaw / Poland.

[2] PhD Candidate, School of Law, Xi'an Jiaotong University, China.

[3] Bachelor's degree, Faculty of Economics daparment of Banking and Finance , Jawzjan University.

| **Received:** 01.02.2026 | **Accepted:** 05.02.2026 | **Published:** 08.02.2026

***Corresponding author: Prof. Dr. Erdal DURSUN**

Rector, International Science and Technology University, Warsaw / Poland.

Abstract

With the rapid expansion of new technologies, especially in the field of artificial intelligence, the structure and traditional methods of armed conflict have changed. The use of intelligent systems in cyberattacks has posed new questions to the responsibility of states for actions taken in cyberspace; especially in terms of attribution of action, proving violations of peremptory norms, and the need to observe fundamental principles of international law such as sovereignty, prohibition of the use of force, and the principle of non-intervention.

This article aims to analyze the legal dimensions of cyberwarfare based on artificial intelligence, while examining the existing frameworks in public international law and the law of armed conflict, and addresses the challenges related to the international responsibility of states.

In this regard, the role of international organizations, existing legal gaps, and the need to formulate new rules are examined in order to provide a solution to enhance legal accountability in the face of new threats.

Keywords: Artificial Intelligence, Cyberwarfare, International Responsibility, International Law, Attribution, Armed Conflicts, Sovereignty of States

Introduction

In recent decades, emerging technologies, especially in the field of artificial intelligence, have significantly shifted the traditional boundaries of international conflicts and interactions. Cyberspace has become one of the main stages of competition and conflict between states; where, without firing a single bullet, vital infrastructure, sensitive information and national security of countries can be targeted.

DOI: 10.5281/zenodo.18523706

These developments have not only transformed the classic concepts of war, but also created fundamental challenges in the field of international responsibility at the legal level. Meanwhile, the use of artificial intelligence in carrying out cyber attacks, due to features such as high speed, independent decision-making and scope of influence, has given the issue more complex dimensions.

Among the fundamental issues are determining the limits of state responsibility for destructive actions in cyberspace, identifying real perpetrators and attributing actions to state individuals or institutions. In such an environment, traditional rules of international law have faced serious questions, the answers to which require a review of existing foundations and the development of new principles. This article seeks to examine and analyze the various dimensions of this legal challenge.

1. Definitions and History

1.1 Definition of Artificial Intelligence

Artificial intelligence refers to a set of technologies and systems that have the ability to perform human-like cognitive tasks, such as learning, reasoning, data analysis, decision-making, and problem solving. Based on extensive data processing and modeling of logical behaviors, these systems are able to perform functions that were previously only possible for humans.

In the military and security field, artificial intelligence is used as a tool for rapid analysis of information, guidance of automated systems, identification of threats and even implementation of cyber operations, and this has raised complex issues in the field of liability and legal control over it (Javadi, Fatemeh Al-Sadat, 2021: p. 62).

1.2 What is cyber warfare and its distinction from other forms of warfare

Cyber warfare refers to a set of offensive or defensive actions in cyberspace that are carried out by governments or their affiliated agents with the aim of damaging critical infrastructure, disrupting information systems, stealing data or weakening the defense and economic capabilities of a country.

Unlike traditional forms of warfare, which are usually accompanied by the use of military force, occupation of territory or physical conflict, cyber warfare is carried out in a non-physical and invisible environment and often appears without clear signs or direct human casualties.

These substantive differences have posed fundamental challenges to identifying the attacker, determining the time of war and applying the classical rules of the law of armed conflict. (Pakzad, Batul: 2011, p. 43)

1.3 A review of the history of the use of technology in modern warfare

With the beginning of the twentieth century, and especially during the First and Second World Wars, technology became a decisive factor in changing the face of war. The use of heavy machinery, aircraft, radar, and finally nuclear weapons showed that the development of technology not only transforms the means of combat, but also military strategies and decision-making methods.

During the Cold War, information and communication technology also became a vital dimension in military competitions between great powers, and new concepts such as electronic and information-based warfare emerged. As we enter the twenty-first century, modern warfare has become increasingly dependent on digital technologies, computer networks, and intelligent systems.

Military operations have gradually expanded into cyberspace, and the scope of threats has also expanded from physical fronts to software, information, and communication infrastructures. Meanwhile, artificial intelligence, as the most advanced technological tool, has played an increasing role in the design, implementation and even decision-making in cyber operations, and this trend has further blurred the boundary between technology and legal responsibility (Aqababayian Damghani et al., 2019, p. 4).

1.4 The entry of artificial intelligence into the field of cyber warfare and its initial legal consequences

The entry of artificial intelligence into the field of cyber warfare is considered a turning point in the evolution of modern conflicts. Today, intelligent systems are able to carry out reconnaissance, infiltration, destruction and even cyber defense operations with high speed and accuracy without direct human intervention. The use of these tools by governments or affiliated agents has led to the formation of a type of conflict that is much more difficult to control, track and contain than traditional forms of war.

In particular, many of these systems are designed to operate autonomously and make independent decisions in certain circumstances. The initial legal consequences of this evolution have affected the system of international responsibility of states with It has raised fundamental questions.

Such as how, in the event of a cyberattack by an AI-based system, the action taken can be attributed to a specific state, or to what extent does the state in question bear responsibility for preventing, controlling, and responding to the destructive actions of such systems.

In a situation where traditional rules of international law are mainly based on human behavior, the introduction of technologies with the ability to make independent decisions has clearly revealed the need to rethink the principles of attribution, responsibility, and accountability (Khalilipour Roknabadi and Noor Alivand, 2012: p. 178).

2. The position of international law in the face of AI-based cyberwarfare

International law, especially in the form of the United Nations Charter and the general principles of customary international law, has provided frameworks for regulating relations between states in peace and war. Principles such as the prohibition of the use of force, respect for national sovereignty, and non-interference in the internal affairs of states constitute the main pillars of this legal system.

However, now, the emergence of cyberwars, especially those conducted with the help of artificial intelligence, has shown that these frameworks are not sufficient to respond to contemporary technological developments. One of the important challenges in this field is to identify instances of resorting to force in cyberspace and determine the starting point of the conflict in the absence of obvious physical violence (Faghih Habibi, Ali, 2016, p. 96).

In addition, international humanitarian law and the rules governing armed conflicts have also faced new questions; including how to implement the principle of separation between military and civilian targets, proportionality in attacks, and observing minimal human

DOI: 10.5281/zenodo.18523706

damage in situations where decision-making has been entrusted to artificial intelligence systems.

Also, challenges such as the lack of transparency in the functioning of these systems and the difficulty in establishing the responsibility of states have severely weakened the international accountability system. Thus, the position of international law in the face of this type of conflict is in a transitional state and requires serious revision and development.

2.1 Fundamental Principles of the United Nations Charter and the Limitation on the Use of Force

The principle of non-use of force, enshrined in Article 2, paragraph 4, of the United Nations Charter, is one of the fundamental principles of contemporary international law and prohibits States from the threat or use of force against the territorial integrity or political independence of other States.

This principle is considered the basis for the maintenance of international peace and security and can only be violated in two limited circumstances: self-defense under Article 51 of the Charter and authorization by the Security Council under Chapter VII.

In the context of AI-based cyber warfare, the main challenge is whether a cyber attack can be considered an instance of "use of force", especially when the attack results in widespread physical damage, human casualties or major disruption of the functioning of critical infrastructure.

In the absence of a clear definition of "force" in the cyber context, the interpretation of this principle in the face of new technologies remains a matter of controversy and various legal analyses (Faghih Habibi, Ali, 2016, p. 90).

2.2 Application of International Humanitarian Law in Cyberspace

International humanitarian law, which is based on the principles of distinction, proportionality, and necessity, has traditionally been used to regulate the behavior of parties in armed conflicts. These laws are designed, especially in classical wars, to prevent harm to civilians and protect civilian targets.

However, in cyberwarfare, given the digital and invisible nature of these attacks, the application of these principles has been challenged. For example, determining what impact a cyberattack has on civilians or whether an attack on a digital network is actually equivalent to an attack on a military target is particularly complex.

Therefore, it is essential that humanitarian law be adapted to cyberspace, and in particular regarding how to deal with systems Artificial intelligence that automatically conducts combat operations should be given more attention (Ebrahimzadeh and Malekizadeh, 2021: p. 86).

One of the main challenges in the application of humanitarian law in cyberspace is the issue of attribution and identification of the parties involved. In cyberwarfare, it is very difficult to determine whether an attack was carried out by a state, a non-state group, or indirect actors.

On the other hand, the concept of "necessity" in cyber operations also needs to be reviewed; because sometimes cyberattacks without any physical damage can severely disrupt the vital infrastructure of countries, which has unpredictable and wide-ranging consequences. Therefore, given the rapid pace of technological progress, the need to develop new laws and procedures to adapt the principles of humanitarian law to the digital space is clearly felt.

2.3 Challenges of identifying the agent in cyber operations mediated by artificial intelligence

In cyberwarfare based on artificial intelligence, one of the fundamental challenges is the accurate identification and attribution of the agent of the attack. Using technologies Advanced technologies such as artificial intelligence (AI), cyber operations can be carried out without the need for direct human intervention or through autonomous systems.

This makes identifying the real perpetrator of an attack more complex than in traditional warfare, where physical and tangible evidence was often available. In cyberspace, attacks may be carried out by a state, non-state groups, or even independent hackers, and these attacks can use distributed and complex networks that make it difficult to trace their origin.

Especially when AI is used in designing cyber attacks, determining the role of humans and institutions involved in the decision-making of those systems becomes a complex issue (Mirbado et al., 2019: p. 249).

Another challenging aspect of identifying the perpetrator is the issue of "masking" or "covert cover" in cyberspace, which can be implemented through advanced techniques such as changing digital signatures, using VPNs, or hidden paths to divert the tracking path.

In these circumstances, even if a cyberattack using AI If the cyberattack is artificial, digital evidence may be completely fabricated or distorted, making it impossible to identify and prove responsibility. These complexities not only complicate the work of intelligence analysts, but also have implications for the legal basis and application of international responsibility. Until these issues are effectively resolved, governments and international institutions will face serious challenges in responding to and responding to cyberattacks.

2.4 Obligations of States to Prevent Cyberattacks on Their Territory

States are obliged, in accordance with the principles of international law, in particular under the Charter of the United Nations and other international agreements, to take effective measures to prevent cyberattacks on their territory. These obligations include establishing and strengthening digital security infrastructures, adopting and enforcing laws related to cybercrime, and cooperating with other States and international organizations to address common threats.

In addition, States should establish effective monitoring and response mechanisms to identify and prevent malicious cyber activities that may emanate from their territory. If States fail to comply with these obligations, they may be considered facilitators of cyberattacks and be held internationally responsible for the consequences thereof. These responsibilities also impose obligations on states to prevent cyberattacks by non-state actors or terrorist groups from occurring on their territory (Mohammad Hosseini et al., 2020, p. 40).

3. International Responsibility of States for Artificial Intelligence-Based Cyberattacks

The international responsibility of states for artificial intelligence-based cyberattacks is one of the complex legal challenges in the era

DOI: 10.5281/zenodo.18523706

of new technologies. According to the principles of international law, states are obliged to prevent their territory from carrying out destructive actions in cyberspace, and since artificial intelligence can design and execute cyberattacks autonomously and without direct human intervention, the responsibility of states in this regard becomes more complex, especially in relation to the use of these technologies.

If a cyberattack is carried out directly or indirectly from the territory of a state or states are unable to control and monitor cyberspace activities on their territory, that state can assume international responsibility for damages caused to another state. This responsibility can include compensation, cessation destructive activities and taking preventive measures to prevent similar attacks in the future.

In this regard, the need to formulate and implement new and transparent legal principles to deal with cyber threats and accurately determine responsibilities is felt more than ever (Rahmati, Reza: 2017, p. 55).

3.1 Elements of International Responsibility (Attributable Conduct and Violation of an International Obligation)

The elements of international responsibility in international law include two main elements: attributable conduct and violation of an international obligation.

a. Attributable Conduct: The first element for international responsibility to occur is that there must be a specific conduct (whether an act or omission) that is attributed to a state or a state entity. This conduct can include positive or negative actions that are directly or indirectly carried out by the state, state officials, or groups affiliated with it. In the context of cyber attacks, if a cyber attack is initiated from the territory of a state or carried out by non-state actors supported by that state, this conduct is attributable to the relevant state. will be attributed (Nemati and Sadeghi Neshat, 2017, p. 170).

b. Breach of an international obligation: The second element is that the imputed conduct is a breach of an existing international obligation. This obligation can arise from various sources, including treaties, international custom, or fundamental legal principles such as the principles of prohibition of the use of force and respect for national sovereignty. If a state violates its obligations to other states, such as preventing cyberattacks or preventing the use of destructive technologies, this breach of obligation will give rise to the international responsibility of that state. In artificial intelligence-based cyberattacks, the violation of these obligations can include failure to monitor cyberspace, failure to prevent destructive activities within its territory, or disregard for cybersecurity obligations (ibid.). These two pillars together create the international responsibility of states for violations of international law and law, especially in the field of cyber threats.

3.2 Direct, indirect and contributory liability in cyber attacks

In international law, the responsibility of states for cyber attacks can be divided into three main categories: direct, indirect and contributory liability. Each of these types of liability has its own characteristics and conditions that are also applicable to AI-based cyber attacks.

a. Direct liability: Direct liability occurs when a state is directly responsible for carrying out or facilitating a cyber attack. These attacks can be carried out directly by state officials or organizations affiliated with them. In this case, the state is clearly responsible for an attack that is under its direct control and direction. For example, if a state uses AI technologies to attack the critical infrastructure of another state, that state is directly responsible. In this type of liability, the attribution of conduct to the state is fully clear and the responsible state must take action to compensate for the damages.

b. Indirect liability: Indirect liability arises when a state is held liable indirectly through supporting or facilitating a cyberattack by non-state groups or individuals. In other words, if a state helps terrorist groups or independent hackers carry out cyberattacks against another state by providing sanctuary, financial resources, training, or technical facilities, that state will be held liable, even if it did not directly carry out the attack itself. This type of liability becomes more complex in AI-based cyberattacks because non-state actors can design attacks using advanced and autonomous technologies without the need for direct state intervention.

c. Collaborative liability: Collaborative liability arises when two or more states jointly play a role in carrying out a cyber attack. In this case, each state is jointly responsible for the cyberattack that resulted from their collaboration. For example, if two states cooperate to design and execute an AI-based cyberattack, both states are jointly responsible.

In this type of responsibility, determining the contribution of each state to the attack and the violation of international law is difficult, especially when complex operations such as cyberattacks combined with AI are carried out. These three types of responsibility, especially in the context of cyberattacks carried out using AI, can lead to serious challenges in determining international responsibility and accountability. Given the existing complexities, there is a need to develop new and clear rules in international law.

4. Legal Requirements and Emerging Challenges in Establishing International Rules

The legal requirements and emerging challenges in establishing international rules in the field of AI-based cyber warfare, especially in the area of state responsibility, are one of the complex and emerging issues in the field of international law. As new technologies, especially AI, are increasingly used in the field of cybersecurity and digital warfare, the need to develop and update international rules to respond to these threats is felt more seriously than ever.

The legal requirements for establishing international rules in this area include the need for a more precise definition of key concepts such as “use of force”, “cyber attack”, “legitimate defense” and “international responsibility” in the cyber world. In this regard, the principles of humanitarian law and other international regulations should be adapted to cyberspace to guarantee human rights and prevent possible abuses (Molavi, Haniyeh, 2023: 18).

DOI: 10.5281/zenodo.18523706

One of the main challenges in setting international rules in this field is the complexity and ambiguity in identifying and attributing responsibility to states and non-state actors. Given the invisible and widespread nature of cyberattacks and the use of artificial intelligence in these attacks, it is very difficult to determine which state or entity is responsible for creating a particular cyber attack.

Also, many principles of international law, such as the prohibition of interference in the internal affairs of states and respect for national sovereignty, may face serious challenges in cyberspace.

In addition, the lack of global consensus on comprehensive rules on cyberwarfare and the responsibility of states can lead to fundamental differences in the interpretation and implementation of these rules at the international level. These problems become a major legal and enforcement problem, especially when artificial intelligence technologies and autonomous algorithms are capable of carrying out complex attacks. (Mostafa Ardebili et al., 2023: p. 89).

4.1 The need to develop specific treaties in the field of artificial intelligence and cyber warfare

The need to develop specific treaties in the field of artificial intelligence and cyber warfare is one of the most important issues that is felt more than ever in today's world and given the rapid developments in new technologies.

Cyber wars, especially when they use artificial intelligence, pose significant challenges to international law. These attacks not only threaten the military and security power of countries, but can also lead to the destruction of vital infrastructure, human casualties, and widespread economic disruptions whose effects exceed any physical war.

In these circumstances, the development of specific treaties to regulate and respond to threats arising from cyber attacks, especially those carried out using artificial intelligence, is extremely necessary (Mirza Aghaei, Mehdi, 2022: p. 43).

Specific treaties can be used in various fields such as determining the responsibility of states for attacks Cyberspace, regulations on the use of artificial intelligence in military operations, and the development of specific rules to prevent the escalation of cyber crises at the international level.

These treaties can help reduce the risks and threats posed by new technologies by creating a common legal framework for the prevention of cyberwars, developing rules related to self-defense in cyberspace, and clarifying the responsibilities of states towards non-state groups. In addition, specific treaties can help create mechanisms for resolving disputes and establishing international supervisory and enforcement institutions in this field.

Also, given the complex and changing nature of cyber threats, these treaties must be flexible and up-to-date in order to be able to effectively coordinate with rapid developments in this field (Zarrukh, Ehsan, 2010, p. 68)

4.2 The role of international organizations and global consensus in setting regulations

The role of international organizations and global consensus in setting regulations related to cyber warfare and the use of artificial intelligence is of particular importance. Due to their transboundary nature and global impact, cyber threats cannot be managed within the borders of a single country and require extensive international cooperation. International organizations such as the United Nations, the International Telecommunication Union, and the Organization for Security and Cooperation in Europe play a key role in developing global standards and regulations.

These organizations are able to adopt principles to prevent cyberattacks, regulate the use of artificial intelligence in wars, and determine the responsibility of states for violations of international law by creating common frameworks and international laws (Jafari, Kamran, 2012: p. 53).

Global consensus is also of great importance in this regard, because in today's digital world, cyber threats and attacks based on artificial intelligence can affect all countries. Without international cooperation and global agreements, it will be difficult to effectively confront these threats.

Achieving global consensus on the development of uniform regulations in this field will help states to take effective and coordinated measures against cyber threats and the misuse of artificial intelligence in wars. As a result, international organizations and global consensus seem essential to create a coherent legal and legal environment.

4.3 Legal Futures in the Face of Rapid Advances in Military Technology

Legal Futures in the Face of Rapid Advances in Military Technology, Especially in the Field of War Cybersecurity and the use of artificial intelligence require analyzing and anticipating potential challenges and developments in the digital and military worlds. Given the rapid development of new technologies, such as autonomous artificial intelligence systems, combat robots, and sophisticated cyberattacks, existing laws and legal regulations may soon be unable to cope with new threats.

In this regard, lawyers and experts should develop new principles and standards to regulate the use of these technologies in wars. Also, attention to the ethical and human dimensions of these technologies, especially in the field of cyberattacks and the role of governments in preventing threats, should be included in the process of developing new laws.

Anticipating the legal future in this field requires international cooperation and global consensus to prevent the creation of legal gaps and possible abuses and to form a comprehensive and coherent legal system to deal with new military threats.

Conclusion

In the face of rapid advances in military technologies, especially in the field of cyberwarfare and the use of artificial intelligence, the need to review international laws and regulations is clearly felt. New threats arising from these technologies can create more complex and pervasive threats than traditional wars, the scope and impact of which are not limited to national borders.

Cyberattacks can widely damage critical infrastructure, financial systems and government services, and in addition, autonomous applications of artificial intelligence in the military field can lead to new complexities in identifying responsibility and determining the role of states in violating international law.

Therefore, it is necessary for the international community, especially international organizations, to act effectively in developing and updating international regulations and specific treaties. International organizations, such as the United Nations and the International Telecommunication Union, have a central role in regulating these regulations and can take steps to reduce cyber

DOI: 10.5281/zenodo.18523706

threats and the misuse of artificial intelligence in wars by providing common legal frameworks.

These regulations can be based on human rights principles and international security standards and specify the responsibilities of states towards cyber threats and digital warfare. Also, emphasizing the principle of prevention and promoting international cooperation in order to monitor cyberspace activities can prevent crises and abuses and facilitate the process of ensuring global security.

Finally, given the complexity and speed of technological developments in the military field, especially in the fields of artificial intelligence and cyberwarfare, it is necessary to formulate specific treaties and establish monitoring and enforcement mechanisms to manage these threats.

International law must continuously adapt to rapid technological changes in order to be able to respond effectively to the threats posed by these technologies. This requires global cooperation and consensus at the international level to prevent any crises and damages resulting from the misuse of advanced technologies.

References

1. Pakzad, Batoul (2011), Cyberterrorism, Tehran: Legal Research Spring 2011 - Special Issue No. 4 Rank: Scientific-Research/ISC (35 pages - from 215 to 249) (To access: https://tinyurl.com/5n7ywtw8
2. Ebrahimzadeh, Pouria; Malekzadeh, Amirhossein (2021), The Position of Preemptive Defense from the Perspective of International Law with an Emphasis on Explaining the International Legal Obstacles to Its Application to Protect Civilians, Journal of International Studies, Issue 70, pp. 100-83. To access: https://tinyurl.com/3wafzrhw
3. Javadi, Fatemeh Sadat (2021), New Technologies and Criminal Law: An Approach to Artificial Intelligence, Publisher. Tehran: Tehran University Press. https://mtlj.usc.ac.ir/
4. Aghababaian Damghani, Hamid Reza; Asgarkhani, Abu Mohammad; Mir Abbasi, Seyyed Bagher, 2019, Journal of Jurisprudence and History of Civilization » Volume 16, Issue 59 (Spring 2019) Jurisprudence and History of Civilization, Volume 5, Issue 1, pp. 1-5 1 For access: https://elmnet.ir/doc/2405915-93612
5. Khalilipour Roknabadi, Ali; Noor Alivand, Yaser, Cyber Threats and Their Impact on National Security, Strategic Studies Quarterly, Issue 2, Year 15, pp. 196-167, 2012. For access: https://tinyurl.com/ynka8949
6. Faqih Habibi, Ali (2016), The Position of Humanitarian Rights in Islam and International Documents, Quarterly Journal of Political Research of the Islamic World, Year 6, Issue 2, pp. 81-103. For access: https://civilica.com/doc/1417725/
7. Mohammad Hosseini, Babak; Hadizadeh, Morteza; Ghafelebashi, Seyed Fahim (2020), Drivers of Sustainable Cyber Service Provision in the Government with Emphasis on Maintaining Security through Artificial Intelligence, Iranian Futures Studies Bi-Quarterly, Fall and Winter 2020 - Issue 9, Rank: B (30 pages - from 36 to 65) (To access: https://tinyurl.com/2nadr8cc
8. Mostafavi Ardebili, Seyyed Mohammad Mehdi; Taghizadeh Ansari, Mustafa; Rahmatifar, Samaneh (2023), The Impact of Artificial Intelligence on the International Human Rights System, Journal of New Technologies Law Fall-Winter 2023 - Issue 8 Rank: A (15 pages - from 86 to 100) (To access: https://tinyurl.com/3y2zww7j
9. Molavi, Haniyeh (2023), Study of the Human Rights Challenges of Artificial Intelligence, Publication Place: Fifth International Conference on Humanities, Law, Social Studies and Psychology, pp. 1-27. To access: https://civilica.com/doc/1685686/
10. Mirbod, Leila; Salimi, Sadegh; Niavaran, Saber; Zamani, Seyed Qasem (2019), Cyberterrorism; Violation of Human Rights and Fundamental Freedoms, Medical Law Quarterly, Summer 2019 - Issue 6 (Special Issue) Rank: Scientific-Research/ISC (17 pages - from 224 to 240) For access: https://tinyurl.com/4t3dr6n5
11. Nemati, Nabi Allah; Sadeghi Neshat, Amir, 2017, Investigation of civil liability arising from data security breaches in cyber threats, Quarterly Journal of Protection and Security Research, Fall 2017 - Issue 23 Classification: A/ISC (30 pages - from 157 to 186) To access: https://tinyurl.com/msdxc5y4
12. Jafari, Kamran (2012), Cyberwarfare in International Law, Master's thesis in International Law, Faculty of Law, Payam Noor University, Tehran Province. For access: https://elmnet.ir/doc/10627298-81251
13. Rahmati, Reza, 2017, Cyberspace and Cybersecurity in International Law, Thesis for a PhD in International Relations, University of Tehran.
14. Zarrukh, Ehsan (2010), Cybercrime, Master's Thesis, University of Tehran. https://tinyurl.com/mr4akt5j
15. Mirza Aghaei, Mehdi, 2022, Criteria for Developing a Social Prevention Code of Cybercrime (Based on National and International Documents), Master's Thesis, Islamic Azad University, Electronics Branch.
16. Dr. Mehmet Uçkaç, PhD, & Prof, Dr. Mohammad Ekram YAWAR. (2025). Systematic Literature Review - Talent Management, Succession Planning and Organizational Sustainability. Içinde GRS Journal of Multidisciplinary Research and Studies (C. 2, Sayı 1, ss. 1-7). GRS Publisher. https://doi.org/10.5281/zenodo.16886511
17. Yawar, M. E., & Amany, S. (2025). The Use of Artificial Intelligence in Teaching History and its Effects on Community Leadership. Akademik Tarih ve Düşünce Dergisi, 12(1), 319-332. https://doi.org/10.5281/zenodo.15618802
18. Ekram Yawar, M., & Qurban Hakimi, M. (2025). Explaining the Digital Health Marketing Model in Gaining Health Welfare Support from Nonprofits. *Acta Globalis Humanitatis Et Linguarum*, *2*(2), 4-28. https://doi.org/10.69760/aghel.02500201
19. Ekram Yawar, M., & Qurban Hakimi, M. (2025). The Impact of Artificial Intelligence Technology on Human Resources Performance in Organizations . *EuroGlobal Journal of Linguistics and Language Education*, *2*(1), 96-108. https://doi.org/10.69760/egjlle.2500013
20. Ekram Yawar, M. (2025). The Impact of Artificial Intelligence on the International Human Rights System. *Acta Globalis Humanitatis Et Linguarum*, *2*(2), 62-78. https://doi.org/10.69760/aghel.02500206
21. Ekram Yawar, M., & Jamil Sharıfy , A. (2025). Exploring Rational Reflections in Artificial

DOI: 10.5281/zenodo.18523706

Intelligence. *EuroGlobal Journal of Linguistics and Language Education*, *2*(2), 4-31.
22. Ekram Yawar, M., & Qurban Hakimi, M. (2025). The Impact of Robots and Artificial Intelligence on Human Resources in the Future. *Global Spectrum of Research and Humanities* , *2*(1), 87-97. https://doi.org/10.69760/gsrh.010120250014
23. Ekram Yawar, M., Abdul Sharify, J., & Abdullah Sadat, S. (2025). A Review of International Policymaking in the Field of Artificial Intelligence. *Global Spectrum of Research and Humanities* , *2*(2), 30-39. https://doi.org/10.69760/gsrh.010120250013
24. Ekram Yawar, M., & Qurban Hakimi, M. (2025). Artificial Intelligence, Management and Organizations. *Global Spectrum of Research and Humanities* , *2*(1), 98-108. https://doi.org/10.69760/gsrh.010120250024
25. Prof, Dr. Mohammad Ekram YAWAR, Dr. Ramazan Ahmadi, Muaiyid Rasooli PhD, & Lec. Abdul Jamil Sharify, Examining Diplomacy for Environmental Sustainability in Interaction with Artificial Intelligence (2025) GRS Journal of Multidisciplinary Research and Studies, Vol-2(Iss-8).88-92
26. Yawar, M. E., & Hakımı, M. Q. (2025). A Review of the Ethical and Legal Challenges of Using Artificial Intelligence in the Health System. Akademik Tarih ve Düşünce Dergisi, 12(1), 307-318. https://doi.org/10.5281/zenodo.15618771
27. Yawar, M. E., & Sadat, S. A. (2025). Problems of Using Artificial Intelligence as a Judge in Legal Proceedings. Akademik Tarih ve Düşünce Dergisi, 12(1), 403-420. https://doi.org/10.5281/zenodo.15627539
28. Rahmaniboukani, S., Qurban Hakimi, M., & Ekram Yawar, M. (2025). Medical Artificial Intelligence and the Need for Comprehensive Policymaking. *Global Spectrum of Research and Humanities* , *2*(2), 60-70. https://doi.org/10.69760/gsrh.010120250018
29. Ekram Yawar, M., Abdul Sharify, J., & Abdullah Sadat, S. (2025). Artificial Intelligence and International Peace and Security. *Acta Globalis Humanitatis Et Linguarum*, *2*(2), 49-61. https://doi.org/10.69760/aghel.02500205
30. Dr. Mehmet Uçkaç, PhD, & Prof, Dr. Mohammad Ekram YAWAR. (2025). Systematic Literature Review - Talent Management, Succession Planning and Organizational Sustainability. Içinde GRS Journal of Multidisciplinary Research and Studies (C. 2, Sayı 1, ss. 1-7). GRS Publisher. https://doi.org/10.5281/zenodo.16886511
31. Jamil Sharify, A., Amany, S., & Ekram Yawar, M. (2025). Knowledge Management Approach to Data Mining Process in Smart Business. *Global Spectrum of Research and Humanities* , *2*(2), 128-140. https://doi.org/10.69760/gsrh.010120250041
32. Dursun, E., Jamil Sharify, A. ., Abdullah Sadat, S., Qurban Hakimi, M., & Ekram Yawar, M. (2025). The Role of New Technologies in the Development of E-Learning (With a View to the Opportunities and Challenges Facing Universities and Higher Education Centers). *Global Spectrum of Research and Humanities* , *2*(2), 99-112. https://doi.org/10.69760/gsrh.010120250020
33. Ekram Yawar, M., Abdul Sharify, J., & Abdullah Sadat, S. (2025). A Review of International Policymaking in the Field of Artificial Intelligence. *Global Spectrum of Research and Humanities* , *2*(2), 30-39. https://doi.org/10.69760/gsrh.010120250013
34. Sharıfy, A. J., & Yawar, M. E. (2024). The Position and Influence of Transformational Leadership on Organizational Culture and Strategies. Akademik Tarih ve Düşünce Dergisi, 11(5), 3737-3748. https://doi.org/10.46868/atdd.2024.842
35. Ekram Yawar, M., & Jamil Sharıfy , A. (2025). Exploring Rational Reflections in Artificial Intelligence. *EuroGlobal Journal of Linguistics and Language Education*, *2*(2), 4-31. https://doi.org/10.69760/egjlle.2500011
36. Ekram Yawar, M., Abdul Sharify, J., & Abdullah Sadat, S. (2025). Artificial Intelligence and International Peace and Security. *Acta Globalis Humanitatis Et Linguarum*, *2*(2), 49-61. https://doi.org/10.69760/aghel.02500205
37. Sharıfy, A. J. (2024). Positive and Negative Effects of Technology on Organization Culture. Akademik Tarih ve Düşünce Dergisi, 11(1), 137-147. https://doi.org/10.46868/atdd.2024.653
38. Sharıfy, A. J., & Yawar, M. E. (2025). Examining the Impact of Transformational Leadership in the Development of Organizational Voice "An Analysis of the Mediating Impact of Information and Communication Technology". Akademik Tarih ve Düşünce Dergisi, 12(4), 215-231.
39. Prof. Dr. M. Ekram. YAWAR, Dr. Muhammed. K., Examining the Legal Status of Clouds in International Law (2025) GRS Journal ofMultidisciplinary Research and Studies, Vol-2(Iss-8).101-106 *(PDF) Examining the Legal Status of Clouds in International Law*. Available from: https://www.researchgate.net/publication/394847292_Examining_the_Legal_Status_of_Clouds_in_International_Law [accessed Sep 11 2025].
40. Ekram Yawar, M., & Jamil Sharıfy , A. (2025). Exploring Rational Reflections in Artificial Intelligence. *EuroGlobal Journal of Linguistics and Language Education*, *2*(2), 4-31. https://doi.org/10.69760/egjlle.2500011
41. Ekram Yawar, M., & Qurban Hakimi, M. (2025). The Impact of Robots and Artificial Intelligence on Human Resources in the Future. *Global Spectrum of Research and Humanities* , *2*(1), 87-97. https://doi.org/10.69760/gsrh.010120250014
42. Ekram Yawar, M., & Qurban Hakimi, M. (2025). The role and importance of ethics in the use of artificial intelligence in medical education and in the diagnosis of chronic diseases. *Acta Globalis Humanitatis Et Linguarum*, *2*(1), 308-314. https://doi.org/10.69760/aghel.02500139
43. Yawar, M. E., & Amany, S. (2025). Impact and Role of Information Technology Application on the Success of Leadership, Organization, Society and Individual. Akademik Tarih ve Düşünce Dergisi, 12(1), 352-364. https://doi.org/10.5281/zenodo.15618840
44. Dursun, E., Jamil Sharify, A. ., Abdullah Sadat, S., Qurban Hakimi, M., & Ekram Yawar, M. (2025). The Role of New Technologies in the Development of E-

DOI: 10.5281/zenodo.18523706

Learning (With a View to the Opportunities and Challenges Facing Universities and Higher Education Centers). *Global Spectrum of Research and Humanities* , *2*(2), 99-112. https://doi.org/10.69760/gsrh.010120250020

45. Ekram Yawar, M., & Amani, A. (2025). Features of international trade contract. *Acta Globalis Humanitatis Et Linguarum*, *2*(1), 276-296. https://doi.org/10.69760/aghel.02500137
46. Ekram Yawar, M., Abdul Sharify, A., & Qasim Fetrat, M. (2025). Review and importance of China's New Silk Road Initiative and the European Union's strategy. *Journal of Azerbaijan Language and Education Studies*, *2*(2), 3-27. https://doi.org/10.69760/jales.2025001007
47. Ekram Yawar, M., & Amani, A. (2025). Review of the World Trade Organization General Agreement on Trade in Services and International Trade in Legal Services. *Acta Globalis Humanitatis Et Linguarum*, *2*(1), 297-307. https://doi.org/10.69760/aghel.02500138
48. Dursun, E., Ekram Yawar, M., & Amani, A. (2025). The Role and Importance of National Economic Law in The International Legal Order. *EuroGlobal Journal of Linguistics and Language Education*, *2*(2), 46-74. https://doi.org/10.69760/egjlle.2500082
49. Prof, Dr. Mohammad Ekram YAWAR, & Dr. Mehmet Uçkaç, PhD. (2025). Study of the Member States of the Economic Cooperation Organization in International Law Based on Trade. Içinde GRS Journal of Arts and Educational Sciences (C. 1, Sayı 2, ss. 75-79). GRS Publisher. https://doi.org/10.5281/zenodo.16886030
50. Prof, Dr. Mohammad Ekram YAWAR, & Dr. Mehmet Uçkaç, PhD. (2025). A Review of the Economic Impact of the 2022 Russia-Ukraine War on the International Economy. Içinde GRS Journal of Arts and Educational Sciences (C. 1, Sayı 2, ss. 69-74). GRS Publisher. https://doi.org/10.5281/zenodo.16886018
51. Dr. Mehmet Uçkaç, PhD, & Prof. Dr. Mohammad Ekram YAWAR. (2025). A Review of Understanding the International Economic Order and World Political Economy. Içinde GRS Journal of Arts and Educational Sciences (C. 1, Sayı 2, ss. 30-33). GRS Publisher. https://doi.org/10.5281/zenodo.16875403
52. Ekram Yawar, M. (2025). Correspondence of Forms in Sales Contracts; Examination of Existing Theories in Legal Systems and Discussion of Their Application to the Contract for the International Sale of Goods. *Global Spectrum of Research and Humanities* , *2*(1), 12-27. https://doi.org/10.69760/gsrh.01012025002
53. Ekram Yawar, M., Dursun, E., Najafov, B., & Matin, A. (2025). The New Silk Road: Economic Importance, Investment, and the Shifting Global Balance of Power. *EuroGlobal Journal of Linguistics and Language Education*, *2*(4), 44-70. https://doi.org/10.69760/egjlle.2504004
54. Ekram Yawar, M. ., Jamil Sharify, A., & Matin, A. (2025). An Overview of International Order and Its Impact on International Political Economy. *Luminis Applied Science and Engineering*, *2*(3), 5-26. https://doi.org/10.69760/lumin.2025003001
55. Matin, A., & Ekram Yawar, M. (2025). Donald Trump: International Economics and Economic Globalization (Economic Policy) . *EuroGlobal Journal of Linguistics and Language Education*, *2*(4), 4-16. https://doi.org/10.69760/egjlle.2504001
56. Matin, A., & Ekram Yawar, M. (2025). A Review of Neoclassical Economics and its Importance. *Porta Universorum*, *1*(5), 24-46. https://doi.org/10.69760/portuni.0105003
57. Ekram Yawar, M., & Matin, A. (2025). A comprehensive overview of the international economy and its positive effects on the global economy. *Acta Globalis Humanitatis Et Linguarum*, *2*(4), 82-104. https://doi.org/10.69760/aghel.0250040004
58. Ekram Yawar, M. ., Jamil Sharify, A. ., & Matin, A. . (2025). A Comprehensive Review of the International Political Economy System (From the Past to the Present). *Global Spectrum of Research and Humanities* , *2*(4), 8-34. https://doi.org/10.69760/gsrh.0250203001
59. Amani, A., & Ekram Yawar, M. (2025). International Trade and Export. *Global Spectrum of Research and Humanities* , *2*(2), 50-59. https://doi.org/10.69760/gsrh.010120250186
60. Ekram Yawar, M., & Amani, A. (2025). Incoterms in International Trade Law . *EuroGlobal Journal of Linguistics and Language Education*, *2*(1), 109-122. https://doi.org/10.69760/egjlle.2500014
61. Dr. Mehmet Uçkaç, PhD, & Prof, Dr. Mohammad Ekram YAWAR. (2025). Studying the Position of International Trade in Exports. Içinde GRS Journal of Multidisciplinary Research and Studies (C. 2, Sayı 1, ss. 13-17). GRS Publisher. https://doi.org/10.5281/zenodo.16886391
62. Yawar, M. E., & Sharıfy, A. J. (2024). The Rights of the Financing Contract in the Field of International Trade with an Emphasis on The Agency Contract. Akademik Tarih ve Düşünce Dergisi, 11(5), 3225-3245. https://doi.org/10.46868/atdd.2024.815
63. Sharify, A. J. & Yawar, M. E. (2023). "Investigating The Impact of International Community Aid on Afghanistan's Economic Policies" International Social Sciences Studies Journal, (e-ISSN:2587- 1587) Vol:9, Issue:118; pp:9501-9518. DOI: http://dx.doi.org/10.29228/sssj.73818
64. Yawar, M. E., & Amany, S. (2025). Correspondence of Forms in Sales Contracts: Examination of Existing Theories in Legal Systems and Discussion of Their Application to the Contract for the International Sale of Goods. Akademik Tarih ve Düşünce Dergisi, 12(1), 197-217. https://doi.org/10.5281/zenodo.15514383
65. Prof, Dr. Mohammad Ekram YAWAR, Dr. Ramazan Ahmadi, Muaiyid Rasooli PhD, & Lec. Abdul Jamil Sharify. (2025). Examining Diplomacy for Environmental Sustainability in Interaction with Artificial Intelligence. Içinde GRS Journal of Multidisciplinary Research and Studies (C. 2, Sayı 8, ss. 88-92). GRS Publisher. https://doi.org/10.5281/zenodo.16902942
66. Yawar, M. E., & Sadat, S. A. (2025). Problems of Using Artificial Intelligence as a Judge in Legal Proceedings. Akademik Tarih ve Düşünce Dergisi, 12(1), 403-420. https://doi.org/10.5281/zenodo.15627539

DOI: 10.5281/zenodo.18523706

67. Prof, Dr. Mohammad Ekram YAWAR, Dr. Ramazan Ahmadi, Muaiyid Rasooli PhD, & Lec. Abdul Jamil Sharify. (2025). In the National and International Policy-Making System: The Place of Environmental Protection. Içinde GRS Journal of Multidisciplinary Research and Studies (C. 2, Sayı 8, ss. 93-100). GRS Publisher. https://doi.org/10.5281/zenodo.16902966
68. Dr. Mehmet Uçkaç, PhD, & Dr. Mohammad Ekram YAWAR. (2025). Examining the Position and Role of Biotechnology in the Development of International Environmental Law. Içinde GRS Journal of Multidisciplinary Research and Studies (C. 2, Sayı 1, ss. 26-36). GRS Publisher. https://doi.org/10.5281/zenodo.16886409
69. Dr. Mehmet Uçkaç, PhD, & Prof, Dr. Mohammad Ekram YAWAR. (2025). Systematic Literature Review - Talent Management, Succession Planning and Organizational Sustainability. Içinde GRS Journal of Multidisciplinary Research and Studies (C. 2, Sayı 1, ss. 1-7). GRS Publisher. https://doi.org/10.5281/zenodo.16886511
70. Dr. Mehmet Uçkaç, PhD, & Prof, Dr. Mohammad Ekram YAWAR. (2025). International Law and Nuclear Right. Içinde GRS Journal of Multidisciplinary Research and Studies (C. 2, Sayı 1, ss. 8-12). GRS Publisher. https://doi.org/10.5281/zenodo.16886386
71. Dr. Mehmet Uçkaç, PhD, & Prof, Dr. Mohammad Ekram YAWAR. (2025). The Status and Provisional Implementation of International Treaties in International Organizations. Içinde GRS Journal of Multidisciplinary Research and Studies (C. 2, Sayı 1, ss. 18-25). GRS Publisher. https://doi.org/10.5281/zenodo.16886404
72. Ekram Yawar, M., Abdul Sharify, J., & Abdullah Sadat, S. (2025). Artificial Intelligence and International Peace and Security. *Acta Globalis Humanitatis Et Linguarum*, *2*(2), 49-61. https://doi.org/10.69760/aghel.02500205
73. Ekram Yawar, M. (2025). Long-Term Change in International Relations. *Porta Universorum*, *1*(2), 13-22. https://doi.org/10.69760/portuni.010202
74. Prof, Dr. Mohammad Ekram YAWAR, & Dr. Mehmet Uçkaç, PhD. (2025). A Review of International Relations and (Civilizational Theorizing). Içinde GRS Journal of Arts and Educational Sciences (C. 1, Sayı 2, ss. 44-52). GRS Publisher. https://doi.org/10.5281/zenodo.16885973
75. Prof, Dr. Mohammad Ekram YAWAR, & Dr. Mehmet Uçkaç, PhD. (2025). In the Theories of International Relations and Geopolitics: The Study of Location (The Concept of Conflict). Içinde GRS Journal of Arts and Educational Sciences (C. 1, Sayı 2, ss. 53-60). GRS Publisher. https://doi.org/10.5281/zenodo.16885993
76. Prof, Dr. Mohammad Ekram YAWAR, & Dr. Mehmet Uçkaç, PhD,. (2025). In the International Foreign Policy of Countries: Soft War of Satellite Networks in Fluidity. Içinde GRS Journal of Arts and Educational Sciences (C. 1, Sayı 2, ss. 61-68). GRS Publisher. https://doi.org/10.5281/zenodo.16886009
77. Mohammad , E. Y. (2025). The Place of Culture in International Relations Theories. *EuroGlobal Journal of Linguistics and Language Education*, *2*(2), 105-123. https://doi.org/10.69760/egjlle.2500191
78. Dr. Mehmet Uçkaç, PhD, & Dr. Mohammad Ekram YAWAR. (2025). Examining the Position and Role of Biotechnology in the Development of International Environmental Law. Içinde GRS Journal of Multidisciplinary Research and Studies (C. 2, Sayı 1, ss. 26-36). GRS Publisher. https://doi.org/10.5281/zenodo.16886409
79. Ekram Yawar, M. (2025). An Overview of Refugee Rights In International Documents. *Global Spectrum of Research and Humanities* , *2*(1), 76-86. https://doi.org/10.69760/gsrh.01012025010
80. Dursun, E., Ekram Yawar, M., & Amani, A. (2025). The Role and Importance of National Economic Law in The International Legal Order. *EuroGlobal Journal of Linguistics and Language Education*, *2*(2), 46-74. https://doi.org/10.69760/egjlle.2500082
81. Dursun, E., Amani, A., & Ekram Yawar, M. (2025). The Legal Framework of the World Trade Organization from the Perspective of Game Theory in International Law. *Global Spectrum of Research and Humanities* , *2*(2), 71-98. https://doi.org/10.69760/gsrh.010120250019
82. Ekram Yawar, M. (2025). Space Grand Strategy in the Light of International Relations Theory. *EuroGlobal Journal of Linguistics and Language Education*, *2*(4), 25-43. https://doi.org/10.69760/egjlle.2504003
83. Ekram Yawar, M. (2025). A Review of the Chinese School of International Relations: Moral Realism. *Acta Globalis Humanitatis Et Linguarum*, *2*(4), 105-128. https://doi.org/10.69760/aghel.0250040005
84. Ekram Yawar, M., Abdul Sharify, A., & Qasim Fetrat, M. (2025). Review and importance of China's New Silk Road Initiative and the European Union's strategy. *Journal of Azerbaijan Language and Education Studies*, *2*(2), 3-27. https://doi.org/10.69760/jales.2025001007
85. Ekram Yawar, M., Jamil Sharıfy , A., & Qasim Fetrat , M. (2025). Review and importance of the Silk Road Initiative; China's initiative for hegemony. *Journal of Azerbaijan Language and Education Studies*, *2*(1), 49-63. https://doi.org/10.69760/jales.2025001005
86. Rasooli, M., Yawar, M. E., Sharıfy, A. J., Haqyar, E. (2024). China-Afghanistan Relations: Change to the Path of Strategic Partnership. Akademik Tarih ve Düşünce Dergisi, 10(6), 2603-2627. https://doi.org/10.46868/atdd.2023.606

DOI: 10.5281/zenodo.18523706