Migration Letters

Volume: 20, No: S6(2023), pp. 234-248

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)
www.migrationletters.com

Applications of Artificial Intelligence in Cybersecurity and its Challenges (Legal analytical study)

Wahaj Ali Hamza[1], Husam Abdul Ameer Khalaf[2]

Abstract

This study explores the applications of artificial intelligence in the field of cybersecurity and its role in ensuring compliance with international law. The first section deals with detailing the applications of artificial intelligence in the field of cybersecurity, pointing to its role in detecting and combating cyber threats and how it can contribute to achieving cybersecurity, in addition to that. The research focuses on how to enhance compliance with international law through these applications and maintain international stability.

The second section addresses the challenges facing the application of artificial intelligence in the field of cybersecurity, and highlights the legal and security challenges, such as issues of privacy and national sovereignty, as well as ethical challenges related to negative use and discrimination.

Overall, this study demonstrates the importance of AI technology in enhancing cybersecurity and compliance with international law, but also draws attention to the importance of dealing with the legal, security, and ethical challenges that accompany using these technologies responsibly and ethically.

Keywords: *Artificial intelligence applications, cyber threats, legal challenges, cyber security.*

Introduction

First: Introducing the subject of the study

Applications of artificial intelligence in the field of cybersecurity are necessary to confront increasing cyber threats, as its uses include massive data analysis, threat detection, traffic filtering, improving application security, and identifying user identities. However, on the other hand, there are technological, legal, and ethical challenges that require consideration, as it is necessary to ensure Data protection, respect for users' privacy, and compliance with laws and ethics in the use of these technologies, and in this regard, we will address this in detail within the framework of the study.

Second: The aim of the study

The primary objective of the study is to explore and analyze the applications of artificial intelligence in the field of cybersecurity and how it can play a role in ensuring compliance with international law, by highlighting the following:

1- Providing a comprehensive understanding of artificial intelligence technology and how it can be applied in the field of cybersecurity.

[1] University of Baghdad, College of Law, Iraq, wahaj.ali1204a@colaw.uobaghdad.edu.iq
[2] University of Baghdad, College of Law, Iraq, dr.hussam@colaw.uobaghdad.edu.lg

2- Study the role that artificial intelligence applications can play in enhancing compliance with international laws and regulations related to cybersecurity.

3- Analyze the challenges facing the application of artificial intelligence in the field of cybersecurity, including legal, security and ethical challenges.

4- Propose solutions and recommendations to overcome these challenges and enhance the use of artificial intelligence applications in enhancing cybersecurity and compliance with international laws.

Third: Problems of the study

Studying the issue of artificial intelligence applications and their challenges faces many legal challenges in the international context. These challenges relate to how modern technology is integrated with security strategies and the technical challenges associated with this application. They also relate to the extent to which these applications are effective in improving compliance with international laws and whether they are able to address legal challenges. The complex

Fourth: Study questions

The problem of the study becomes clear by answering the following questions:

1- What is the technology used in artificial intelligence applications in the field of cybersecurity?

2- How can artificial intelligence applications help organizations ensure compliance with international law in the field of cyber?

3- What are the legal and security challenges facing artificial intelligence applications in the field of cybersecurity?

4- What are the ethical challenges associated with using artificial intelligence technology to combat cybercrime?

Fifth: Study plan

According to the above, this topic was divided according to a methodological plan that includes two sections according to the following:

The first topic: Applications of artificial intelligence in cybersecurity and its role in ensuring compliance with international law.

- The second topic: Challenges of applying artificial intelligence in the field of cybersecurity.

In conclusion, we will review the most important conclusions and recommendations reached in accordance with our integrated vision on the subject.

The first topic

Applications of artificial intelligence in cybersecurity and its role in ensuring compliance with international law

Cyber crimes and wars have become)It poses a real threat to countries, organizations, and individuals at the present time, because once they are connected to the Internet, all their information stored on electronic devices will be vulnerable to hacking, theft, espionage, and other illegal acts that constitute crimes, whether war crimes or crimes of aggression.)It causes huge financial losses and severe damage at the international level, and for this reason several countries were forced to search for ways to defend their cybersecurity against these internationally illegal acts through the use of applications based on smart technologies.

Therefore, in this research, we will discuss, in the first requirement, artificial intelligence technology and its applications in the field of cybersecurity, and in the second

requirement, the role of artificial intelligence applications in enhancing compliance with international law in the field of cybersecurity.

The first requirement

Artificial intelligence technology and its applications in the field of cybersecurity

In the modern digital age, artificial intelligence technologies have an increasing role in various fields, including the field of cybersecurity, and applications of artificial intelligence in the field of cybersecurity aim to protect systems and data from electronic threats and cyberattacks, and among these applications are the following:

First: Program Microsoft Defender

Prepare Microsoft Defender is one of the programs used to protect against viruses and malware and relies on artificial intelligence techniques to detect cyber threats And limit it, and it has been used in many countries of the world. In 2019, the US Department of Defense announced its adoption ofMicrosoft Defender for the purpose of protecting its government computers This declaration indicates its commitment to an international rule that states must take all necessary measures and means to protect cybersecurity and develop them to prevent cybercrime This rule was mentioned in several international agreements, especially the Budapest Convention against Cybercrime, which was signed by the member states of the Council of Europe in 2001, and which in its preamble encouraged the necessity of developing information and communications technology and using it in this regard It is a programMicrosoft Defender is one of the tools that can be used in this field.

Second: Electronic platforms

It is a platform Indicative of electronic platforms Which adopts artificial intelligence techniques for the purpose of combating cyber threats, by analyzing data and behavioral patterns of users and devices connected to the network to detect any security threats that may face the organization or country that uses it, and there are many countries and organizations that have resorted to using it as a means to protect their cyber security, sensitive data, and vital government information. Of hostile cyber threats, foremost among which is the United States of America, as in 2020 the US Department of Homeland Security launched a partnership withIndicative to enhance its capabilities for early detection of cyber attacks and improve the security of its cyber system.

In addition to "Indicative", there are other platforms that use artificial intelligence techniques in the field of combating cyber threats, for example the "Cylance" platform, which was developed to detect and prevent cyber attacks, and Cylance uses deep learning and artificial intelligence techniques to analyze the behavior of files and malware and determine whether they pose a threat. security)

There is also a platform Insight Vulnerability Management, is the result of a collaboration between the US General Services Administration and Rapid7 The United States of America is one of the countries that uses this technology to defend itself against cybercrime. It has used artificial intelligence and information security techniques to identify loopholes and secure government systems, and a platform has been applied. Insight Vulnerability Management debuted in 2018 to enhance vulnerability detection and vulnerability management capabilities in US government systems.

In short, these electronic platforms represent examples of how artificial intelligence technologies can be used to combat cyber threats, and they contribute to improving information and data security for countries and organizations.

Third: Applications plunk

It is a smart application mainly used in the fields of cybersecurity, records and incident management, as it is distinguished by its ability to analyze huge data collected from

various sources, including system and network logs, performance reports and other data sources to extract valuable information effectively and at a low cost. It is also used in.. Analyze incident data, verify cyber attacks, and track hackers. In addition, it is used to analyze system and network logs to identify problems and improve system performance. The data is stored in a database.Splunk, which facilitates the process of accessing it and using it for analysis. In practice, we find that this application has been used in many countries of the world, including the United States of America, the United Kingdom, Japan, Canada, and Australia. Its use depends on the need to analyze big data and detect cyber attacks in each country.

Fourth: Application Symantec Endpoint Protection

It is one of the most prominent cybersecurity applications that uses artificial intelligence techniques to detect and reduce malicious programs. This application is distinguished by its ability to learn behavioral models of systems and networks, and to automatically analyze security data to detect any threats. Several countries have used it in their government systems, including the United States. America, Britain, France and other countriesFor example, in 2019, France used the Symantec Endpoint Protection application in a campaign to combat malware and other security threats targeting the French security defense system.

According to the above, we find that by using artificial intelligence applications in the field of cybersecurity, countries and organizations are able to effectively protect their systems and data from increasing cyber threats and achieve the highest levels of cybersecurity, which enhances regional and international stability.

However, on the other hand, there are some dual-use applications that were created primarily to measure the effectiveness of cyber defense efficiency, but at the same time they can be exploited negatively at times. We mention, for example,Metasploit, which is a powerful tool that relies on artificial intelligence and machine learning techniques to test the security of networks and systems, and provides a wide range of tests to identify vulnerabilities and evaluate the integrity of systems. It also allows professionals in the field of cybersecurity to conduct penetration tests legally and systematically, as it can be used to discover vulnerabilities and exploit them. To access systems and achieve specific testing objectives, the advanced capabilities of artificial intelligence in Metasploit also allow improving testing processes and vulnerability analysis, which helps in identifying weak points and enhancing the security of systems, but at the same time it can be used to penetrate systems and obtain confidential information. In 2016, it was It was used to carry out a cyber attack on the German Parliament, and the attackers were able to obtain sensitive data and important government information, causing the computers to be disabled.)And disrupting government systems in the country, and it was later revealed that the attack was carried out by parties related to the Russian government.

There are alsoJohn the Ripper is a smart application used to test the strength of passwords and decrypt encrypted data. It is distinguished by its ability to carry out powerful attacks to test the strength of passwords used in a specific system. The application also uses artificial intelligence and data analysis techniques to improve its ability to break and decrypt passwords. Passwords in effective ways, and its work depends on experimentation and guessing techniques to test passwords in different ways. The application also analyzes the speed of experimentation and the strength of the passwords used and provides detailed reports and analyzes.

However, this application can also be used for illegal purposes such as hacking computers and stealing sensitive information for a country or organization, and one of the countries that was subjected to cyber attacks using this application is the United States of America in 2015, as the US National Security Agency (NSA)Hacking by a group of hackers calling themselves “Shadow” used this application in the attack to hack passwords and control the agency’s internal network.

As forTHC Hydra is a popular program in the field of information security and penetration testing. It is used to test the strength and penetration of systems and evaluate the effectiveness of passwords. It is also used in security testing operations to verify the strength and protection of cloud systems, web servers, networks, access management systems, and many other systems. THC Hydra is characterized by With its ability to carry out experimental attacks, the program works by trying a large group of potential passwords using trial and error techniques to find the correct password and penetrate the system, but at the same time it gives attackers the ability to test passwords and penetrate computer systems that use weak or easy passwords. guess A good example of this application is the attack on a companySony Pictures Entertainment in 2014, which was carried out by a group of hackers belonging to North Korea. Security investigations later revealed that the hackers used an applicationTHC Hydra tried millions of passwords and guessed them, and eventually succeeded in penetrating some of the company's computer systems. This attack led to the leaking of many sensitive information and documents, and created a wave of criticism and controversy about data security and privacy on the Internet

The second requirement

The role of artificial intelligence applications in enhancing compliance with international law

Artificial intelligence technology plays an important role in enhancing compliance with international law in the field of cybersecurity, as international law in this field governs the behavior of states and individuals in virtual space It aims to protect cyber assets and maintain the stability of the international system. Below we will explain how artificial intelligence applications can contribute to enhancing compliance with international law in the field of cybersecurity:

First: predictive analysis and early warning

Through predictive analysis and early warning, artificial intelligence applications contribute to enhancing compliance with international law, as artificial intelligence technologies are characterized by their ability to deal with huge amounts of data and enhance network security by building autonomous security systems to identify various attacks and respond to violations, as receiving a large number of Security alerts on a daily basis can pose a major challenge for security teams, and through automatic intrusion detection and response, the efforts required by security experts can be reduced and the efficiency in identifying threats can be increased more than other techniques.

In fact, when huge amounts of security data are generated and transmitted over the network every day, it becomes very difficult to quickly and reliably track and identify it by network security experts, so artificial intelligence helps expand the scope of monitoring and identifying suspicious activities, and this can help network security experts. In response to new situations, time-consuming manual analysis methods can be replaced.

From the above, we find that applications of artificial intelligence contribute to enhancing compliance with international law through predictive analysis of risks and illegal behaviors, as by using deep learning and data analysis techniques, artificial intelligence can analyze big data and identify patterns and behaviors that are not in compliance with international law and based on these Expectations: Institutions and companies can take precautionary measures and strengthen their systems and policies to comply with international laws. For example, artificial intelligence applications can be used to detect money laundering and the financing of terrorist organizations. and other illegal activities, which helps prevent and monitor illegal activities and contribute to enhancing compliance with laws.

Also, artificial intelligence applications can monitor ongoing cyber threats and analyze strategic models and trends in the cyber field. This can be done by monitoring and analyzing network traffic and identifying suspicious patterns and new threats. Artificial intelligence can also analyze data from previous attacks and draw conclusions. Attack models and methods used. Using this information, artificial intelligence can identify weak points in systems and networks, direct security enhancement efforts, and develop cyber defense strategies. Strategic analysis based on artificial intelligence can also help identify the main targets of attacks and predict future attack patterns, enabling organizations to Taking early measures for prevention and defense, and then it can be said that artificial intelligence applications contribute to enhancing compliance with international law by analyzing threats and strategic analysis.

The cybersecurity response to detect threats depends on comprehensively monitoring application behavior and network activity over time, as the security system identifies regular movement and behavior in the network, and creates a database of normal behavior, and through this it is possible to monitor any deviations from this rule and detect attacks, Modern technologies constitute a new field of research that enhances security measures in the cyber field, and many artificial intelligence methods are used to deal with threats, including computational intelligence, neural networks, intelligent agents, artificial immune systems, data mining, pattern recognition, and reasoning. Machine learning, deep learning, etc. Among these technologies, machine learning and deep learning are famous for their achievements in combating cyber threats.

From the above, we find that artificial intelligence applications help enhance cybersecurity and compliance with international laws through their ability to enhance the ability of countries to deal with attacks and threats effectively and immediately. Artificial intelligence techniques such as machine learning and software robots can also be used to confront complex cyberattacks and implement.. Appropriate cyber defense measures. Artificial intelligence can also be used to develop strong verification and authentication systems, and update them continuously to protect systems from hacks and attacks that violate the rules of international law.

Second: Developing cybersecurity policies and legislation

Artificial intelligence applications can play an important role in developing cybersecurity policies and legislation at the international level. One of the main benefits of using artificial intelligence in this context is the ability to analyze data and information related to cyberattacks in smart and effective ways. By analyzing this data, artificial intelligence applications can Identifying gaps in the cybersecurity infrastructure and identifying patterns of attacks and targeted threats to existing security systems. This would work to strengthen the infrastructure and not make it a clear target for all illegal terrorist cyber attacks in accordance with the European Convention for the Suppression of Terrorism and the Protocol attached to it, which was adopted in 1977

It then provides smart recommendations regarding enhancing protection and developing strategies to respond to new threats. In addition, artificial intelligence applications can contribute to analyzing existing laws, identifying gaps in them, and submitting proposals to strengthen the legal framework related to cybersecurity. Based on the analysis of legal data, effective policies and legislation can be developed. Responds to cybersecurity challenges and enhances countries' ability to protect critical systems and information from cyber threats.

Third: directing policies and making decisions

Artificial intelligence can be useful to governments in the field of analyzing cyber data and understanding the international contexts of cyber security incidents, and this would contribute to formulating national policies and making strategic decisions to enhance cyber security. For example, artificial intelligence can help in analyzing patterns of cyber

attacks and identifying Who is responsible and what tactics are used, enabling governments to develop effective response strategies and take appropriate precautionary measures).

Fourth: Developing defense technologies

Smart technologies can be effectively exploited in developing defense technology with the aim of enhancing compliance with international laws. For example, artificial intelligence can play a vital role in enhancing compliance with international laws through the development of intrusion detection systems and advanced monitoring systems, thanks to its ability to analyze unusual behaviors in systems. Information technology can detect intrusions faster and more accurately than traditional technologies, and this improvement in efficiency means that cybersecurity can be better achieved and violations of international laws in the field of cybersecurity prevented. Therefore, artificial intelligence can contribute significantly to enhancing compliance with international laws by enhancing Cybersecurity and preventing illegal intrusions.

Sixth: Supporting investigation operations

Artificial intelligence can play a crucial role in enhancing compliance with international laws in the field of cybersecurity by supporting investigations and legal procedures. Thanks to the development of technology and the ability to process large amounts of digital data, artificial intelligence can effectively process and analyze electronic data to discover evidence related to cybercrimes. Such as hacking and electronic fraud.

It can also provide advanced analytics to help authorities identify the sources of attacks and cybercrimes and help them track down the perpetrators.

add to that, The results of analyzes and data provided by artificial intelligence can be used as strong legal evidence in trials, contributing to enhancing justice and ensuring that those involved in illegal activities on the Internet are punished.

In this way, AI can have a positive impact on enhancing compliance with international laws in the field of cybersecurity by supporting investigative processes and providing the evidence necessary to achieve justice.

From the above, we find that artificial intelligence can play a decisive role in enhancing compliance with international laws in the field of cybersecurity through predictive analysis and early warning of threats, developing cybersecurity policies and legislation, guiding policies and decision-making, developing defensive technologies, and supporting investigation operations, and this It contributes to enhancing cybersecurity and preventing cybercrimes, which contributes to maintaining international stability and preserving the electronic security of countries and institutions.

The second topic

Challenges of applying artificial intelligence in the field of cybersecurity

Although artificial intelligence, when used correctly, has the potential to revolutionize the field of cybersecurity and improve the overall security of countries and organizations alike, as is the case with any new technology, its use in this field would raise a number of challenges. The legal and ethical issues that must be addressed in order to ensure that the use of artificial intelligence applications is compatible with the requirements of international law. Within the framework of our topic, we will discuss the most prominent challenges raised by the use of artificial intelligence in the field of cybersecurity.,Which are as follows:

The first requirement

Legal and security challenges

The use of artificial intelligence in the field of cybersecurity raises a number of challenges at the international level, and these challenges are represented in the following:

First: ambiguity and lack of legal rules

The use of modern smart technologies in the field of cybersecurity faces great challenges at the international level, the first of which is the absence of international legal rules regulating some of the issues resulting from the use of artificial intelligence in the cybersecurity of countries. For example, the issue of determining the "scope of artificial intelligence" from an international legal perspective is difficult due to the lack of A fixed legal framework to regulate the use of smart technologies in the field of cybersecurity. This situation leads to certainty about the legal repercussions of the use of technologies based on artificial intelligence, which hinders their development and raises the concerns of countries and organizations about their use, in addition to the issue of the independence of artificial intelligence as an explicit challenge to international law Especially with regard to the issue of international responsibility If any damage occurs as a result of the use of smart technology, who bears international legal responsibility in this case? Is the country using artificial intelligence, or the facility Which developed the program used for artificial intelligence, or even the manufacturer of the robot or device that used artificial intelligence, or the country in which the facility is located. Artificial intelligence can also make automated decisions without human intervention, and this would also raise questions about international legal responsibility in the event Any damage occurs due to these decisions. This also makes it easier for the actor to evade international responsibility and hold the technology accountable because it is independent in its decisions based on Article (II) of the report of the International Law Commission on the work of its fifty-third session, which acknowledges that international responsibility is limited only On actions issued by state agencies or persons who acted in accordance with instructions issued by its agencies or by order or under its supervision, that is, they have the status of an agent for the state Therefore, clear international rules must be established to regulate the use of smart technologies, especially in the field of cybersecurity, and countries and organizations must work together to define the legal responsibilities of the parties concerned with the optimal use of this technology.

Likewise, at the national level, we find multiple and different legislations that address artificial intelligence, which leads to differences in definitions of terms, responsibilities, and required procedures. Therefore, these legislations and standards must be unified to achieve effective regulation of the use of artificial intelligence in cybersecurity.

Second: Damage to information privacy and individual rights

The use of smart surveillance systems, such as video cameras, electronic cards, personal data bases, and means that monitor mail, communications, the work environment, etc., to process personal data comes with potential risks that affect the rights of individuals The International Court of Justice also confirmed that there is complementarity between human rights and international law, which is the basis for protecting these rights Given that these systems have high powers and unlimited capabilities in dealing with information, these risks include losing data, destroying it, modifying it illegally, disclosing it to unauthorized parties, or processing it illegally, and this makes sensitive information more vulnerable to hacking. And illegal use, which leads to an attack on the individual's rights to privacy in violation of the International Covenant on Civil and Political Rights, which prohibits interference with the privacy of individuals.

For this reason, some countries hesitate to use artificial intelligence to protect their sensitive information from hackers for fear of endangering their privacy. To avoid this,

we find it necessary to make regional and national efforts to protect the right to privacy, enact legislation, and focus on finding a balance between the need of countries to collect and store personal data and ensuring the protection of this data. The risks of illegal use of these smart systems.

Third: Increase in cyber attacks

Increasing the ability of conflicting parties to use smart technologies in cyber attacks constitutes a major challenge in the field of cyber security. Although smart technologies can be used to enhance cyber security, they can also be used by attackers to develop and implement more sophisticated and complex attacks. When.. The ability to use smart technologies in cyber attacks increases, along with the ability of attackers to exploit security vulnerabilities more effectively and carry out advanced attacks such as hybrid attacks that combine traditional cyber attacks with artificial intelligence techniques.

To address this challenge, cybersecurity teams and security stakeholders must take preventive and precautionary measures to enhance cybersecurity and combat smart threats. These entities must also enhance their ability to use smart technologies to detect advanced attacks and threats and respond to them quickly and effectively.

Fourthly: Algorithmic bias

There is another type of challenge that will need to be addressed as the use of artificial intelligence in cybersecurity grows: algorithmic bias. By certain countries to develop the artificial intelligence systems they possess against the cybersecurity of another country, as algorithms are used to analyze and interpret data using pre-defined rules, which raises serious questions about their legal validity, which makes them inherently biased according to the country that set the rules of these algorithms, and this would violate The United Nations Charter, which stipulates respect for the principle of equality among all peoples, and that algorithmic bias would lead in the future to creating a digital gap between developed countries that have striven to organize their technological capabilities and made them a key element in maintaining their cybersecurity, and those other countries that It aspires to achieve its cybersecurity according to the available capabilities, as it will be divided accordingly into strong countries that possess advanced technologies that can penetrate the cybersecurity of any country that stands in its way, and weak countries that do not possess any of these technologies and thus will be under the control of the strong state because it cannot confront it.and its compliance with those developed countries).

Fifth: ThreatDigital sovereignty

Digital sovereignty) (It is a concept that refers to the state's right to control and control its data and cyber system, and when using artificial intelligence in cybersecurity, some challenges arise regarding the state's sovereignty over this data, and among these challenges is the dependence of many artificial intelligence techniques on training models and algorithms using data sets. Huge data, so the state needs to ensure that there is sufficient cyber data available to train its models, and providing this data may sometimes be a challenge and requires cooperation with private ICT companies.

Also, relying on artificial intelligence algorithms in cybersecurity may require improved capabilities to process and analyze data quickly and effectively, and this may require the use of powerful data centers or servers and modern technology that may not be available to all countries alike. The use of artificial intelligence can also lead to.. In cybersecurity, some sensitive security functions are transferred to smart systems and machines. Which poses a challenge to the state in maintaining sovereignty and full control of these functions, and therefore the state needs to develop appropriate policies and laws to ensure that critical security decisions are not made without the necessary human review.

The second requirement

Ethical challenges

It is important to realize that the use of technology in general, and artificial intelligence in particular, carries ethical risks if it is not dealt with seriously and responsibly, and among the most prominent ethical considerations related to the use of artificial intelligence are:

Firstly:Prejudice and non-discrimination

Data discrimination and bias are two important issues related to the ethics of using artificial intelligence technologies in different fields. Discrimination is manifested in the unfair or unequal treatment of individuals' data, while bias is manifested in making specific decisions or actions based on that data.

Data discrimination may occur when personal data is collected from certain groups without adequate consideration for diversity or fairness in the use process. For example, if data is collected from a specific group or geographic area, other groups and diverse social and cultural circumstances that may affect data may be ignored. Analyzing and interpreting that data, this can lead to bias in the results and making unfair decisions.

On the other hand, ethical bias can occur when smart technologies are used to make decisions that favor one group over another based on misinterpretations or unfair discrimination. For example, artificial intelligence may be used to analyze records of individuals' cyber activity and make decisions based on patterns extracted from this data, if This data suffers from discrimination in its collection or classification, which may lead to unfair decisions being made towards specific categories of individuals such as racial, sexual or religious minorities The 2018 Toronto Declaration on the Protection of the Right to Equality and Non-Discrimination in Machine Learning Systems indicated the necessity of ensuring justice, equality, and non-discrimination in the design of the smart system. It also required that it be designed in a way that ensures equality among all users, regardless of gender, race, or Color, religion, creed, nationality, social or economic status, age, disability, or any other factors, and advertising highlights an important issue, which is that discrimination can occur when data is collected unfairly or when smart algorithms are used that rely on distinguishing between individuals based on some factors obtained from their data) .

Therefore, the designers and developers of the smart system must be careful in designing the system in a way that ensures that there is no discrimination against any person or group, and that standards of justice and equality are followed in all aspects of the system's design, development and use.

Second: The difficulty of achieving a balance between technological progress and human safety

Developing artificial intelligence technology in a way that protects humanity would constitute an important challenge facing the international community at the present time. Despite the great benefits that the use of artificial intelligence can bring in multiple fields such as medicine, industry and technology, the most important main challenges are ensuring that Artificial intelligence is designed and used in a way that protects humanity and maintains the principles of ethics, human values, and safety. Therefore, everyone must deal with these challenges responsibly and adhere to international standards related to safety. A clear example of efforts to achieve this balance is the petition to postpone the training of more powerful artificial intelligence systems.GPT-4 for a period of 6 months, and the application of international standards related to safety in the use of technology. This petition was signed by many business leaders and experts in the field of technology, led by Elon Musk, on March 29, 2023, which indicates their keenness to achieve safety and responsibility in developing technology. artificial intelligence In order to achieve this important goal, the international community, governmental and private organizations

must cooperate together in this regard, in addition to launching more initiatives and projects aimed at developing artificial intelligence technologies in a sustainable and responsible manner, and encouraging cooperation between organizations, individuals and communities, which can help achieve balance. Required.

Third: Lack of transparency and issue

The use of artificial intelligence in the field of cybersecurity requires providing sufficient transparency regarding how it is used and how decisions are made based on that data, as well as holding developers and users responsible for using the technology and any negative repercussions that may arise from it.

In addition, the values of democracy and the rights of individuals must be strengthened when using smart technology and controlling their personal data and ensuring that personal data is not used illegally or unwanted. It is necessary to commit to providing tools supported by artificial intelligence to ensure privacy and implement the General Data Protection Regulation, as it should The use of artificial intelligence is beneficial, and the process of its development and use does not violate basic human rights, in a way that enhances social welfare and security, in addition to proving the credibility and reliability of technology systems and their developers, the necessity of using technology in a sustainable manner, and enhancing awareness of the impact of the use of technology on the environment and the economy.

Fourth: Weak ethical standards and controls

The use of artificial intelligence in the field of cybersecurity raises many important ethical issues, and among these issues is determining the necessary ethical decisions when facing cyber attacks. In some cases, the artificial intelligence system may be required to make a decision to destroy or nullify a cyber attack. This means that it must determine what priorities are and how to evaluate potential harms. This issue conflicts with other complex ethical issues, such as the issue of determining life and property, as there may be a conflict between protecting personal interests and public interests. For example, a system may have intelligence. Artificial intelligence has the ability to destroy offensive devices, but this may lead to significant loss of human life or cause irreversible damage.

To solve these ethical challenges, stakeholders and developers must work together to define appropriate ethical standards and controls for the use of artificial intelligence in the field of cybersecurity. A legal and ethical framework must be established that regulates the use of artificial intelligence in this field. In addition, mechanisms must be included for making ethical decisions and ensuring the evaluation of.. The potential harms and benefits accurately. In addition, experts should participate in the legislative and regulatory process to determine the basic principles that the artificial intelligence system must follow in making ethical decisions. Mechanisms for interpreting ethics must also be included in the design and development of artificial intelligence systems used in the field of security. Cyber, and these mechanisms can include principles and guidelines that define the values and ethical standards necessary to make difficult decisions.

Conclusion

At the conclusion of this topic, we reached a set of conclusions and recommendations, which we will clarify as follows:

First: conclusions

1- Cybersecurity is a set of procedures and measures that aim to protect electronic systems and digital information from a variety of threats. Cybersecurity also works to

maintain the confidentiality of information and data integrity and ensure the sustainability of services across networks and digital systems.

2- The technology used in artificial intelligence applications in the field of cybersecurity includes a variety of technologies such as machine learning, artificial neural networks, behavior analysis, and pattern recognition. These technologies are used to monitor and detect cyber threats faster and more accurately.

3- Artificial intelligence applications contribute to ensuring compliance with international law in the field of cyber by enhancing the ability to track and analyze illegal cyber activities and determine responsibilities. They can also be used to provide strong and reliable legal evidence in cases of cyber attacks.

4- The legal and security challenges facing the applications of artificial intelligence in the field of cybersecurity include issues such as protecting data privacy and compliance with local and international legislation, and challenges are also faced with regard to addressing the misuse of artificial intelligence in cyber attacks.

5- The ethical challenges associated with the use of artificial intelligence technology in combating cybercrime include several issues such as the negative use of personal data and privacy espionage, as organizations must ensure that these technologies are used in an ethical and balanced manner so that they do not violate the rights of individuals.

Second: Recommendations

1- Organizations and governments should invest in research and development in AI technologies to enhance their cybersecurity.

2- We hope that individuals and institutions understand that technology is not a final solution, and that new ways to confront cyber threats must always be sought.

3- The need for governments and institutions to strengthen international cooperation to develop international standards and laws that regulate the use of technology and artificial intelligence in the field of cybersecurity.

4- The international community must understand that cyber challenges require a unified international response and are not just an issue for individual countries

5- The need to enhance training and education in the field of cybersecurity and cyberlaw to enable professionals to face the increasing legal and security challenges.

6- We hope that governments and institutions will be ready to adapt to rapid technological developments and ensure compliance at all times.

References

First: legal books

1- Ahmed Muhammad Barak, Towards Regulating the Rules of Responsibility for Artificial Intelligence Technologies, Wael Publishing House, first edition, 2022.

2- Peter B. Sale, The Digital Universe, the Global Revolution in Communications, translated by Dhia Warad, Hindawi Foundation, first edition, 2021.

3- Stuart Russell, Human-Compatible Artificial Intelligence, translated by Mustafa Muhammad and Fouad Ismail, Hindawi Foundation, first edition, 2022.

4- Adel Abdel Sadiq, Personal Data: The Struggle over Twenty-First Century Oil, Arab Center for Cyberspace Research, 2018.

5- Alaa Abdel Razzaq Al-Salmi, Introduction to Cyber Artificial Intelligence, Arab Organization for Administrative Development, League of Nations, first edition, 2022.

6- Omar Makki, International Humanitarian Law in Contemporary Armed Conflicts, International Committee of the Red Cross, 2019.

7- Lectures by Asmaa Nouri and Muhammad Abboud entitled Digital Portals and Platforms, Al-Mustansiriya University, Department of Information and Libraries, 2021.

Second: Theses and dissertations

1- Omar Nafi Reda, The Legal System for Artificial Intelligence, A Comparative Study, Master's Thesis, College of Law, University of Mosul, 2021.

Third: Scientific journals

1. Ahmed Al-Shouri Abu Zaid, Artificial Intelligence and the Quality of Governance, Journal of the College of Economics and Political Science, Volume 23, Issue 4, 2022.

2. Ahmed Al-Shouri Abu Zaid, Artificial Intelligence and the Quality of Governance, Journal of the College of Economics and Political Science, Volume 23, Issue 4, 2022.

3. Report of the International Law Commission on the work of its fifty-third session to the General Assembly, Volume 2, Part 2, 2001.

4. Gegan A. Sh. (2022). The cyber impact on the national security of active countries (the United States of America) as a model. Journal of Political Science, (64), 1–18.https://doi.org/10.30907/jcopolicy.vi64.628.

5. Hamid A. Kh. (2019). The phenomenon of terrorism and human rights violations after 2001. Journal of Political Science, (54), 215–230.https://doi.org/10.30907/jj.v0i54.38.

6. Al Khatri, Rashid, and Zayed Ali. 2023. "Recruitment of people into terrorist organizations, its techniques and methods - UAE law as a model." Journal of Legal Sciences 38(1):84-106.https://jols.uobaghdad.edu.iq/index.php/jols/article/view/638.

7. Behind Hossam Abdel Amir. 2019. Integration between international criminal law and international humanitarian law in combating terrorism. Journal of Legal Sciences 31(4): 187-222.https://doi.org/10.35246/jols.v31is. .

8. Daham, Muhammad, and Mahmoud Khalil. 2022. "The Legality of and International Responsibility for the Use of Cyberattacks in International Conflicts." Journal of Legal Sciences 36(4): 678-704.https://doi.org/10.35246/jols.v36i4.520.

9. Sabrina Magnani and Moghaddam Shabila, The role of big data in supporting sustainable development in Arab countries, Journal of Information Studies and Technology, Volume 4, Issue 1, 2019.

10. Salah, Mahdi and Hadi Al-Maliki. 2023. "The Preference of Peremptory Norms in Public International Law." Journal of Legal Sciences 38(1):128-66.https://jols.uobaghdad.edu.iq/index.php/jols/article/view/641.

11. Abdel Amir, Ahmed. 2023. "Legal Protection of Computer Software." Journal of Legal Sciences 38(1):649-73.https://doi.org/10.35246/jols.v38i1.618.

12. Al-Maliki Hadi Naeem and Abdel Mustafa Salem. 2017. "The Spatial Scale of War Operations in International Armed Conflicts." Journal of Legal Sciences 31 (4): 28-57.https://doi.org/10.35246/jols.v31is.100.

13. Muhammad, Sun, and Bayda Wali. 2023. "International Responsibility to Repel Boat Refugees." Journal of Legal Sciences 38(1):731-47.https://jols.uobaghdad.edu.iq/index.php/jols/article/view/663.

14. Mahmoud Lama Abdel Baqi and Kaitan Israa Nader. 2021. "International Liability for Damage Caused by Cyber Attacks." Journal of Legal Sciences 36 (December): 336_362.https://doi.org/10.35246/jols.v36i0.435.

15. Mukhaled Ibrahim Al-Zoghbi, The Effectiveness of Arab Laws and Legislations in Confronting Cybercrime, Arab Journal for Scientific Publishing, Issue Thirty-Seven, 2021.

16. Muslim Nibras Ibrahim. 2017. "War Crimes and Crimes of Aggression in the Jurisprudence of the International Court of Justice." Journal of Legal Sciences 31(4): 223-46.https://doi.org/10.35246/jols.v31is.107.

17. Mona Turki Al-Musawi, Information privacy, its importance, and the dangers of modern technologies to it, Journal of the Baghdad University College of Economic Sciences, Special Issue of the College Conference, 2013.

18. Nazim Hassan Rasheed, Auditing Bias in Artificial Intelligence in Light of the Institute of Internal Auditors' Artificial Intelligence Auditing Framework _Analytical Theoretical Study_, Journal of Contemporary Business and Economic Studies, Volume 6, Issue 1, 2012.

19. Nabil Muhammad Abdul Rahman Haider, Controlling the slopes of highway lines using artificial intelligence with applications to the city of Riyadh, King Saud University, Riyadh, 2000.

20. Younis Malih, Digital Sovereignty in Morocco... Its Manifestations and Possibilities of Achieving It, Middle East Journal for Legal and Jurisprudential Studies, Volume 2, Issue 2, 2022.

Fourth: Laws and announcements

1. Budapest Convention against Cybercrime 2001.

2. International Covenant on Civil and Political Rights of 1966.

Fifth: Foreign sources

1. Anandita Iyer And Umadevi, Role of AI and Its Impact on the Development of Cyber Security Applications, 1ST Edition 1, 2023.

2. Anne Boily, Tensions in the Artificial Intelligence (IA) A hermetic guide for political studies, these doctors, University of Montreal, 2020.

3. Betsy Page Sigman, Erickson Delgado and others, Splunk: Enterprise Operational Intelligence Delivered, packt publishing, 1st edition, 2017.

4. Denitsa Kozhuharova, Atanas Kirov and others, Cybersecurity of Digital Service Chains, Springer, volume 13300, 2022.

5. Frederik Zuiderveen Borgesius, Intelligence Artificielle et Decisions Algorithmiques, Direction générale de la Democratic Conseil de l'Europe, Strasbourg, 2018.

6. Haibo He and Jun Yan, Cyber-physical attacks and defenses in the smart grid: a survey, IET Cyber-Physical Systems: Theory & Applications, Volume 1, Issue 1, 2023.

7. John Ray And William Ray, Mac OS

8. Lee Allen, Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide, Packt Publishing, 2012.

9. Marta Stroppa, Legal and ethical implications of autonomous cyber capabilities: a call for retaining human control in cyberspace, Springer, Volume 25, Issue 1, 2023.

10. Rajneesh Gupta, Hands-On Cybersecurity with Blockchain, Packet Publishing, 1st edition, 2018.

11. Robert Walters, Marko Novak, Cyber Security, Artificial Intelligence, Data Protection & the Law, Springer, 2021.

12. Sagar Samtani and Maggie Abate, The Palgrave Handbook of International Cybercrime and Cyberdeviance, 1ST Editions, 2020.

13. Stuart McClure, Joel Scambray and others, Hacking Exposed 7: Network Security Secrets and Solutions (Hacking Exposed), McGraw Hill Publishing, 7th Edition, 2012.

14. Teresa Rodríguez de las Heras Ballell, Legal challenges of artificial intelligence: modeling the disruptive features of emerging technologies and assessing their possible legal impact Get access Arrow, Uniform Law Review, Volume 24, Issue 2, 2019.

15. Thanh Cong Truong and Quoc Bao Diep, Artificial Intelligence in the Cyber Domain: Offense and Defense, Symmetry, Volume 12, Issue 8.

16. Usman Tariq and Irfan Ahmed, A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review, Sensors, Volume 23, Issue 8, 2023.

17. Will Gragido And John Pirc,"Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats, 1st Edition.

18. Yuri Diogenes And Erdal Ozkaya, Cybersecurity - Attack and Defense Strategies, Packt Publishing, 1st edition, 2018.

19. Fanoos, H. Q., & Bkeet, APMSA (2022). Deterritorialized States Within the Framework of Public International Law. Resmilitaris, 12(1), 282-295

Sixth: Electronic sources

1. Considerations for End-Users,P.5. ,file:///C:/Users/hp/Downloads/Khelkala_etal_AI_based_COs_and_Ethics%20(4).pdf .Date of visit: 4/21/2023, at 1:08 pm. https://www.torontodeclaration.org/wpcontent/uploads/2019/12/Toronto_Declaration_Arabic.pdf Date of visit: 4/20/2023, at 5:47 AM, .

2. Kirsi Helkala,James Cook And Other,AI in Cyber Operations: Ethical and Legal

3. Symantec Endpoint Protection, https://www.symantec.com/products/endpoint-protection. Date of visit: 4/18/2023, 1:00 PM,

4. Toronto Declaration: Protecting the right to equality and freedom from discrimination in machine learning systems. The document can be viewed through the following link.: https://www.torontodeclaration.org/wpcontent/uploads/2019/12/Toronto_Declaration_Arabic.pdf Date of visit: 4/20/2023, at 5:47 AM.