Information Sciences Letters

Volume 12
Issue 7 *Jul. 2023*

Article 56

2023

AI Techniques for Combating Electronic Crimes and Enhancing Cybersecurity: Kuwaits Security Services as a Model

Nassereldin A. Osman
College of Mass Communication, Ajman University, Ajman, United Arab Emirates, t.abdellatif@ajman.ac.ae

Mohammad M. Alshammari
Saad Al- Abdullah Security Sciences Academy, Kuwait, t.abdellatif@ajman.ac.ae

Tarek I. Mohamed
College of Mass Communication, Ajman University, Ajman, United Arab Emirates, t.abdellatif@ajman.ac.ae

Recommended Citation

A. Osman, Nassereldin; M. Alshammari, Mohammad; and I. Mohamed, Tarek (2023) "AI Techniques for Combating Electronic Crimes and Enhancing Cybersecurity: Kuwaits Security Services as a Model," *Information Sciences Letters*: Vol. 12 : Iss. 7 , PP -.
Available at: https://digitalcommons.aaru.edu.jo/isl/vol12/iss7/56

Information Sciences Letters
An International Journal

http://dx.doi.org/10.18576/isl/120756

AI Techniques for Combating Electronic Crimes and Enhancing Cybersecurity: Kuwait's Security Services as a Model

Nassereldin A. Osman[1], *Mohammad M. Alshammari*[2], *and Tarek I. Mohamed*[1,*]

[1]College of Mass Communication, Ajman University, Ajman, United Arab Emirates
[2]Saad Al- Abdullah Security Sciences Academy, Kuwait

Received: 5 May 2023, revised: 21 Jun. 2023, Accepted: 28 Jun. 2023
Published online: 1 Jul. 2023

Abstract: The research aimed to examine the security agencies' use of artificial intelligence (AI) techniques in combating cybercrime and its reflection on enhancing cyber security. The study used the survey method in its descriptive and analytical levels. The interview tool was used to collect information from the research sample, the size of which was 12 items. The research found a set of results where the respondents declared the presence of an anti-cybercrime team comprised of specialists in police sciences, engineering, information systems, and network engineering. They added that using AI enables specialists in security agencies to benefit from its enormous potential in analyzing data, tracking cybercrime perpetrators through social networking sites, managing, and using information, following up on complaints, publications, and other messages, preparing security reports, and submitting them to the competent authorities, completing many general daily tasks and monitoring all the information that may affect the public opinion. The study recommended setting up industries related to AI technology to produce smart knowledge and unifying Arab capabilities in the information technology and communication field to protect Arab national security by combating foreign technical intrusions and virtual hegemony, representing the most advanced form of futuristic weapons.

Keywords: Security Agencies – Artificial Intelligence - Cybercrime - Cyber Security- Electronic Crimes.

1 Introduction

Cybercrime has been associated with the advent of the information age and computers. It has become one of the simplest and most common types of crimes during the current time. The spread of this crime may pose a threat to the conservative Gulf society; it may affect its economy, national security, and social fabric by defaming individuals, publishing incorrect sources, spreading false news and rumors, using text messages and phone calls maliciously to facilitate heists and harm national security. Given recent technological developments, the term "intelligence" has become widespread in many fields, including combating cybercrimes, and various techniques have emerged to track these crimes. Security agencies have recognized the importance of using more skills to track these crimes, which highly skilled persons do to invade others' privacy and facilitate security breaches, resulting in threatening the integrity of states, destabilizing governments, and mounting economic troubles. So, these agencies have resorted to using artificial intelligence technologies to counter cybercrime, which has been linked to research tools, comments management, and data analysis techniques to maintain public security.

Using AI techniques has become an urgent need owing to various factors, including high rates of dependence on the internet and social networking sites, abuse of these sites by some individuals and groups to commit cybercrimes, and these crimes' severe impacts on states' security and safety.

These techniques provide societies with a security benefit by enabling security officials to save time creating lists, scheduling meetings, and sending Emails, and empowering them to perform their security duties more actively [1].

This research examines the security officials' use of artificial intelligence (AI) techniques in combating cybercrime and its impact on strengthening cyber security in Kuwaiti society.

2 Research definitions:

-Artificial Intelligence: It is the science and engineering domain concerned with the theory and practice of developing systems that exhibit the characteristics we associate with intelligence in human behavior [2]. Here, it is determined in the intelligent software underlying the programs and technologies used by security officials through websites that help

[*]Corresponding author e-mail: t.abdellatif@ajman.ac.ae

rapidly create content and data tracking.

-Cybercrime is crimes committed online using the computer as a tool or a targeted victim. Classifying crimes in general into distinct groups is challenging as many crimes evolve daily. However, all cybercrimes involve both the computer and the person behind it as victims. It just depends on which of the two is the main target. Hence, the computer will be considered a target or a tool for simplicity's sake [3]. This research determines the crimes against individuals and the government; the anti-individual crimes include identity theft (impersonation, emails, and accounts theft) to falsely implicate a person, distort his image, and hide the identity of the criminal and the criminal process. In contrast, anti-government attacks include attacking official websites, government systems, and networks locally or internationally, such as electronic terrorist attacks aiming to destroy infrastructure and attack computer networks.

-Cyber warfare is the art and science of fighting without fighting, of defeating an opponent without spilling their blood [4]. Here, the direct link between national security and AI is determined here because information power has become the most crucial factor in the state's power situation, especially after the AI technology revolution. It is used to describe sabotage campaigns, shutdowns, and electronic wars.

-Cyber security is a technique generally outlined in published materials to safeguard a user's or organization's cyber environment. It manages the methods to save the integrity of networks, programs, and data from unauthorized access. It refers to the body of technologies and processes and may also be referred to as information technology security. The field is increasingly important due to increasing reliance on computer systems, including smartphones, televisions, and the various tiny devices that constitute the Internet of Things. Internet-connected systems, including hardware, software, and data, from cyber-attacks are protecting them. In a computing context, security comprises cyber and physical security. Enterprises use both to protect against unauthorized data center access and other computerized systems. Security, designed to maintain data confidentiality, integrity, and availability, is a subset of cyber security [5]. Here, it means the procedures and efforts made by security officials to enhance cyber security by combating cybercrimes that harm the state's national security.

3 Research importance:

- Examining the most prevalent types of cybercrime in Kuwaiti society and their impact is essential.
- The importance of determining the motives of committing cybercrime and the methods used.
- The increasing security concerns about the spread of cybercrime in the last decade and its danger to national security.
- The growing threat of cybercrime dangers which become equivalent to risks in real life.
- The marked scarcity of studies and research on using AI techniques in combating cybercrime at the Arab level.
- The necessity to conduct more studies on the security agencies' use of AI techniques in combating cybercrime.

4 Research objectives:

The research aims to examine the security agencies' use of artificial intelligence (AI) techniques in combating cybercrime and its reflection on enhancing cyber security.

5 Research questions:

- Are there specialists in combating cybercrime? What are their qualifications and experience?
- What are the most prevalent cybercrimes in the Gulf society? What are the risks posed by these crimes?
- What are the essential tools used in committing cybercrime?
- How do AI technologies affect combating cybercrime?
- What are the experts' and specialists' most important proposals contributing to enhancing cyber security in Kuwait?

6 Previous Studies

6.1. AI Technologies

In recent years, there has been a new wave of reflection on and criticism of artificial intelligence (AI) technologies' theories and principles in society's everyday life. The massive penetration of AI technologies in people's lives raises various conceptual and methodological issues for sociology and, more generally, social sciences. The development of AI technologies appears to be a prominent aspect of contemporary social change. Because it is embedded in and influenced by different social practices, it cannot be adequately understood from a single professional standpoint or disciplinary framework [6]. Humanity is undergoing the most unprecedented changes in its history due to modern technologies. Human interactions, relationships, and behavior patterns have changed, and society depends entirely on machines, which have become an integral part of our lives [7]

Digital transformation strategies are based upon four core dimensions, including the technology used to achieve the government's strategic role and support its future vision, changes in value creation strategy, structural changes, and other financial aspects of digital transformation [8]

It is essential to consider the effects of AI on every facet of society. It has helped to facilitate many businesses in various fields, including media, and provided the possibility to solve issues quickly and effectively. Also, it has had a growing role in journalism, affected the journalistic routine favorably, and helped to expand coverage [9] rapidly.

6.2. AI and Media

AI has affected the media; many jobs and tasks may disappear, and robots may carry out journalistic tasks. However, AI technologies could never replace the human brain shortly, and humans will remain the supervisors of using AI to do work quickly, accurately, and more effectively [10]

In using AI for journalism practice, its impact is confirmed regarding three elements: contents, forms, and professional personalities [11]. Modern communication means have imposed several changes on the five phases of the journalism production process (news gathering, verification, validation, visual and editorial processing, publishing, and feedback), directly affecting the newsrooms' products and services [12]

The AI role has grown in recent years to affect news production processes and support the media content industry by obtaining, evaluating, and processing information quickly [13]. The media organizations which do not adopt AI technologies will face an extremely bleak future [14].

This technology will support journalists rather than be a substitute for them. Although the growing concerns about AI threaten journalism, it has offered ample opportunity to facilitate journalistic activities by helping with information-processing tasks, creating news stories, and providing broad coverage to broad readers. Also, AI has successfully improved leadership skills and managerial decision-making by enhancing the speed and accuracy of decisions, relying on high-quality predictions and proven facts [15]. Finally, AI will minimize interpersonal contact, reduce the workload, and make tasks more complex and challenging [16].

So, modern technology has an apparent effect in developing traditional newsrooms into rooms that adopt appropriate strategies aligning with the digital age. Media organizations are keen to take advantage of the most important modern technologies to keep pace with these changes through new strategies that help them to integrate with technology and maintain their survival. On the other hand, AI has ethical and legal challenges determined by the lack of transparency, accountability, and safeguards, illustrating the importance of evaluating its due legal process [17].

Also, AI has many disadvantages, including its high cost, complications, and unclear legal responsibility [18]. Moreover, it drives us to an uncertain future due to the rapid development of robotics and continuous improvements in machine learning [19]. Humans should be prepared to deal with this technology, and a seventh sense needs to be developed to understand the complex technical challenges between intelligent humans and innovative machines.

7 Theoretical framework

7.1. Technological Determinism (TD) Theory

The technological theory of the media is one of the modern theories related to the role of the media and its impact on various societies. It is one of the most widespread media theories that believe in the importance of media and communication technologies in shaping communities rather than media content. It is the idea that technology has significant effects on our lives.

The theory was first instituted by Marshall McLuhan, a professor of English at the University of Toronto in Canada and one of the most famous intellectuals during the second half of the 20th century. He argued that the media content could not be viewed in isolation from the technology of the media tool. Also, he saw that the media organization's method of presenting topics and the targeted audience direct its messages. He proposed that mediated technologies ensure culture diffusion in a society, which helps to change human behavior. He stated, "We shape our tools, and they, in turn, shape us" [20].

For McLuhan, media is a more robust and explicit determinant than the more general concept of language. As a more moderate version of media determinism, he proposed that our media use may subtly influence us. Still, more importantly, the social context of use is crucial [21].

McLuhan saw that the fundamental shift in technological communication leads to significant transformations, not only in the social system but also in human sensitivity. He considered that media content determines the social order, and we can't understand the method of media work without understanding the social and cultural changes that occur in societies. He added that any given technology's effects depend to some extent on the social context, and this context will encourage or discourage the technology's adoption. If the technology is adopted, the social context will have important effects on how the technology is used and thus on its ultimate impact [22].

Although we do not fully agree with this theoretical concept, we recognize it is consistent with the effects of the fifth revolution of communication due to how people use new media and AI applications in combating cybercrime [23].

7.2. AI Techniques for Cybersecurity by Security Agencies.

There are several examples of electronic crimes that AI can help combat, including:

- Identity theft: AI can help detect and prevent identity theft by analyzing patterns of user behavior and identifying anomalies or inconsistencies.
- Phishing attacks: AI can identify and block phishing emails to steal sensitive information from individuals or organizations.
- Fraudulent transactions: AI can be used to identify and flag suspicious transactions, which can help prevent financial fraud and money laundering.

Malware attacks: AI can detect and prevent malware attacks, including ransomware, which can cause significant damage to computer systems and networks.

8 Research Methodology

The research used the survey method in its descriptive and analytical levels. Data for this study was collected personally by the authors using in-depth interviews. This information-gathering tool includes conducting a lengthy and in-depth personal interview with the respondents to answer the research questions; for qualitative research, which is looking for open answers that are not previously known (not closed), as in the case of a questionnaire that includes pre-expected answer choices.

The population of the study was made up of AI experts and officials in the Department of Public Security in Kuwait due to the tight security measures taken by security forces. A sample size of only 12 respondents was determined, and the respondents were asked to remain anonymous.

9 Research results:

9.1. The experience and skills of AI specialists:

The respondents declared the presence of an anti-cybercrime team, made up overwhelmingly of specialists in police sciences, engineering, information systems, and network engineering. They added that AI and its advanced potential had provided new challenges to the state national security system because of the accelerating technological capabilities that no human can deal with in the future. They assured us that failure to face this technical transformation would take us out of the digital age progresses.

9.2.The most prevalent cybercrimes at present:

The respondents determined these crimes as follows:

- **Financial crime:** It is one of the most common crimes facing the financial sector in the Gulf States. It is run by significant international gangs specialized in bank account theft through hacking.
- **Personal cybercrime** is a form of identity theft in electronic communications related to email accounts and passwords. It includes impersonation and stealing personal information from targeted devices, such as messages, recordings, emails, pictures, and files, to threaten and extortion.
- **Cybercrime against official websites** attacks governments' official websites and network systems to destroy their infrastructure. People who commit this crime are called pirates and often have nefarious purposes.

- **Cybercrime against properties** attacks personal, governmental, and private organizations to destroy important documents and special programs. It is carried out by transferring malicious programs to the targeted devices using harmful emails and virus messages.
- **Security Cybercrime**: It targets sensitive sites of the state to steal information related to the state and its security.

9.3. Threat of cybercrime:

The respondents indicated that cybercrime leads to:

- Family disintegration and disputes among people due to defamation, dissemination of false information, stealing individuals' files and photos, and publishing them on the Internet and social media sites.
- Compromising the national economy and security as well as threatening the social fabric.

1.4. The most used cybercrime tools:

The respondents determined these tools in backup software. These telephone lines are used to connect cameras and spy devices, digital code-scanning tools, bar-code, printers, mobile devices, fixed phones, and stealth software technologies.

9.5. Uses of AI techniques in combating cybercrime:

The respondents argued that using AI can save the time security officials spend on their security activities, such as creating to-do lists, scheduling meetings, sending emails for follow-up, customization, and security meetings. They added that using AI enables specialists in security agencies to benefit from its enormous potential in analyzing data, tracking cybercrime perpetrators through social networking sites, managing, and using information, following up on complaints, publications, and other messages, preparing security reports, and submitting them to the competent authorities, completing many general daily tasks and monitoring all the information that may affect the public opinion.

10 Conclusion:

There is no doubt that cyber security has a vital role in addressing the challenges and risks that threaten state and citizen security, involving espionage, cyber terrorism, electronic piracy, media penetration, and intellectual, cultural, and psychological invasion. With AI, the state becomes more capable of achieving strategic balance using technological capabilities that help identify potential threats and competing lawless groups at the internal and external levels to protect its national security.

Furthermore, the fight against cybercrime will significantly change due to technological developments and scientific discoveries in the coming years. Therefore, AI will occupy an important position as a new and effective technique. Findings show that AI technologies will provide new opportunities to create new jobs in Gulf society, such as software developers, electronics engineers, specialized mechanical engineers, programming specialists, international law experts, data analysts, cyber security experts, financial planners, personal advisors, and network marketing consultants.

Though AI applications are used in security, they can deal with environmental problems, such as climate change and ecological disasters; they can monitor water and air pollution, reduce energy consumption, minimize waste, and expand natural and renewable energy use.

11 Proposals of experts and specialists to enhance cyber security:

Respondents suggested the following:

- Holding more training courses in the technical field, exploring the experiences of others on using AI technology in combating cybercrime, and hosting professionals to benefit from their expertise.
- Adding a course on AI for police cadets and specialized institutes students and promoting this course as a cross-cutting theme in Kuwait university programs.
- Relying on AI in carrying out various security activities and using the latest devices that work with ultraviolet rays and face recognition technology.
- Setting up industries related to AI technology to produce smart knowledge.
- Paying attention to the importance of technology in promoting our existence, freedom, resources, and national security without limiting it to entertainment.
- Reducing the technological gap between Arab and developed countries because it has become an imminent danger

to Arab national security.

- Unifying our capabilities for serious investment in AI in all sectors because there is a strong relationship between the technical and political, economic, and security dimensions.
- Benefiting from Arab scientific cadres to establish a comprehensive project to awaken Arab determination and inspiration in smart technology, technical sciences, and digital applications.
- Unifying Arab Countries capabilities in the information technology and communication field to protect Arab national security by combating foreign technical intrusions and virtual hegemony, which represent the most advanced form of futuristic weapons.
- Establishing an integrated Arab project to protect Arab identity in all its components.
- Providing the infrastructure for the new technologies to bridge the sizeable technological gap in this field depends on cooperation between Arab academics, exchange of experiences, and mobilization of resources and capabilities.
- Intellectuals, philosophers, scientists, researchers, scientific research centers, universities, academic institutions, and all concerned sectors must work to develop an ethical and strategic vision that serves as a binding charter for the people who use, develop, and produce this smart technology to ensure the use of it for the benefit of our societies, communities, and future generations.
- Protecting data from irrelevant access because cyber-attacks on the state's vital system and economic base aim to achieve geopolitical dominance. There is a risk of destabilizing local economies and social structures by hacking state databases to leak, sell, analyze, encode, and redirect information. So, cyber warfare has become an integral part of war tactics between states using soft power.

Acknowledgments

The authors would like to express their profound appreciation for Ajman University – UAE for its support and funding.

Conflict of interest

The authors declare that there is no conflict regarding the publication of this paper.

References:

[1] G. Panda, A. Upadhyay, & K. Khandelwal, "Artificial Intelligence: A Strategic Disruption in Public Relations". *Journal of Creative Communications,* p. 129. (2019).

[2] G. Tecuci, "Artificial intelligence." *Wiley Interdisciplinary Reviews, Computational Statistics*, 4(2). DOI:10.1002/wics. P. 200, (2012).

[3] J. Aghatise, "*Cybercrime definition." Institute of Human Virology, Nigeria*. (PDF) Cybercrime definition (researchgate.net), (2006).

[4] J. Carr, "Inside cyber warfare." 2nd ed., *O'Reilly Media Inc.* p. 242. (2012).

[5] P. Seemma, S. Nandhini, & M. Sowmiya, "Overview of Cyber Security". *International Journal of Advanced Research in Computer and Communication Engineering,* Vol. 7, Issue 11. (2018).

[6] A. Rezaev & N. Tregubova "Artificial Intelligence and Artificial Sociality: New Phenomena and Challenges for the Social Sciences." *Monitoring of Public Opinion: Economic and Social Changes, No. 1.* https:// doi.org/10.14515/monitoring.2021.1.1905. (2021).

[7] S. Shahbi, B. Muhammad, & H. Crouch. "Artificial Intelligence between Reality and Hope: A Technical and Field Study." *International Forum on Artificial Intelligence*: A New Challenge to Law, Algeria, November p. 26-27. (2018).

[8] R. Al-Shishi. "Digital transformation strategy in Egypt and ways to enhance artificial intelligence applications." Research paper*, Faculty of Politics and Economics, Suez University.* P 145. (2019).

[9] A. Sultan, "Artificial Intelligence with Big Data and Cognitive Computing: Opportunities and Threats," *Journal of Science and Technology,* Issue 124. (2019). S. Saad, & T. Issa, "Integration or Replacement: Journalism in the Era of Artificial Intelligence and Robot Journalism." *International Journal of Media,* Journalism and Mass Communications (IJMJMC), Volume 6, Issue 3, (2020).

[10] M. Tunez, "Impact of Artificial Intelligence on Journalism: transformations in the company, products, contents and professional profile." Research paper, *Communication & Society*, vol.34, p. 233. (2020).

[11] O. Abu Arqoub, "The model of the smart newsroom and its use of modern means of communication" *Al-Jazeera Arabic and English newsroom"*. Al-Jazeera Media Institute. (2019).

[12] B. Tousignant, "A Hybrid Analysis of the state of automated journalism in Canada: Current Impact and Future Implications for Journalists and Newsrooms," *Unpublished Master's Thesis*, Montreal, Quebec, Canada, Concordia University, Department of Journalism. P 205. (2020),

[13] B. Javed, "Success Factors in Artificial Intelligence (AI)-Focus on use of Al in Journalism". *Unpublished master's thesis*, University of Applied Sciences, Business Administration (MBA). P. 110. (2020).

[14] W. Ali, & M. Hassoun, "Artificial Intelligence and Automated Journalism: Contemporary Challenges and new opportunities". *International journal of media, journalism and mass communications (IjMJMC),* Volume 5, Issue 1, p .207. (2019).

[15] M. Van der Meiji, "The Impact of Artificial Intelligence on workplace tasks in an internal user support Environment an explorative cross-case Study from the Perspective of internal user support staff." *Unpublished Master's Thesis*, School of Industrial Engineering, Science Innovation Management.p. 244 (2018).

[16] H. Boutghan, & N. Ben Kasher. "Pioneering Journalism and the Future of Digital Newsrooms: A Prospective Study." May 8 University, *Faculty of Humanities and Social Sciences*, Department of Information and Communication Sciences and Library Science, Guelma, Algeria. (2017).

[17] C. Beckett, "New Powers, new responsibilities A global survey of Journalism and artificial intelligence." Research paper, (Lse) *the London school of economics and political science.* (2019).

[18] S. Samiei, "On the Danger of Artificial Intelligence." Unpublished Master's Thesis, Auckland, *School of the Engineering University of Technology.* P. 167. (2019).

[19] A. Jan, Shakirullah, S. Naz, O.Khan, & Q. Khan, "Marshal Mcluhan's Technological Determinism Theory in the Arena of Social Media". *Asers publishing,* Vol 11 No 2. DOI: https://doi.org/10.14505/tpref.v11.2(22).00 (2020).

[20] M. McLuhan. "Understanding media: the extensions of man". *1st ed., McGraw-Hil*l, New York. P 232. (1964).

[21] P. Simon. "Technological Determinism." *The International Encyclopedia of Organization Studies*, edited by Stewart Clegg and James R. Bailey (Sage). (2006)

[22] B. Baya & W. Bin Trad, "Theoretical frameworks explaining networked media between effectiveness and limitation.*" Maalem Journal for Media and Communication Studies,* Volume One, Issue One, Faculty of Information and Communication, University of Algiers, Joan. P. 75. (2020).