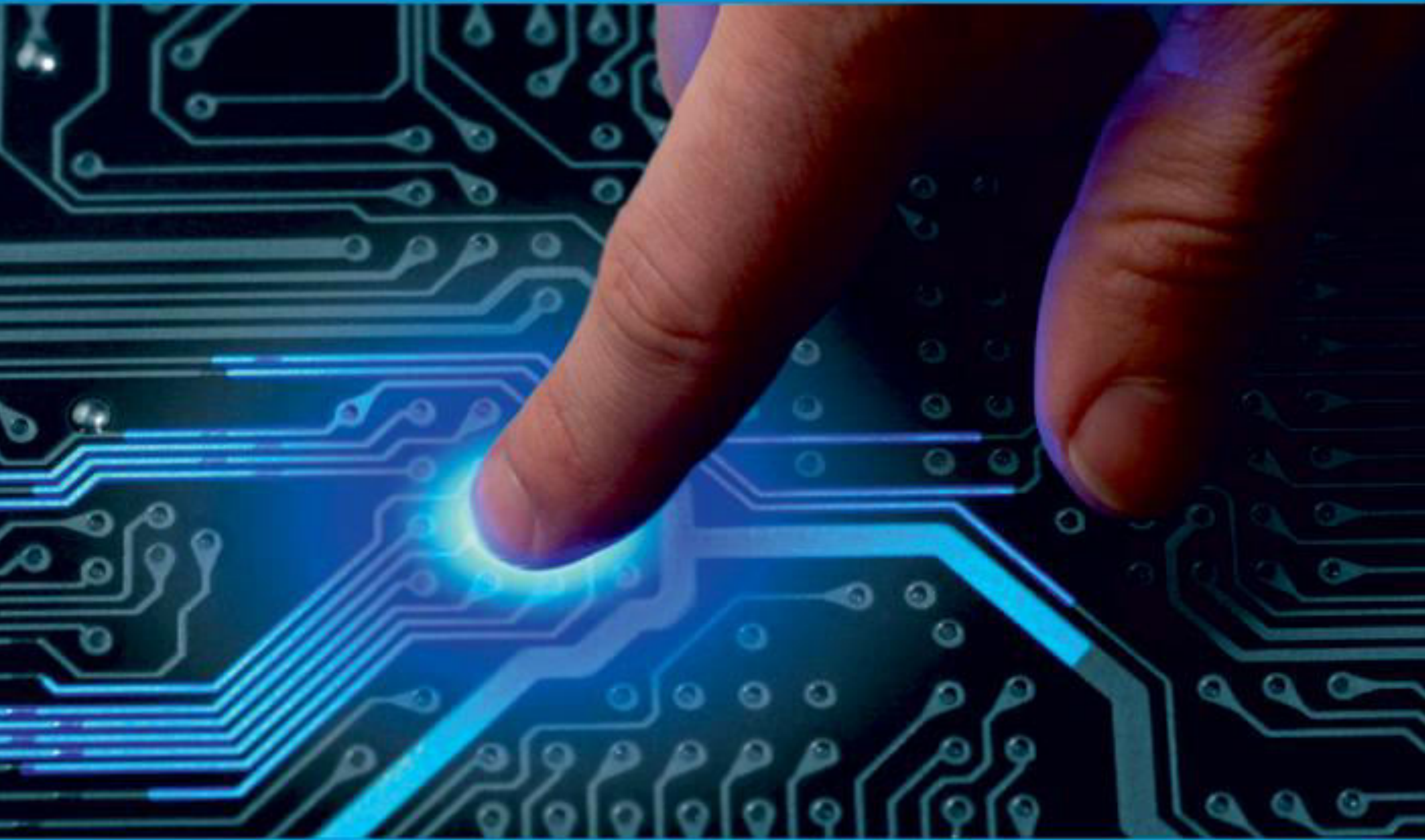
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203044 |

The Role of Artificial Intelligence in Cyber Security

Vasanth M, Murugan R

PG Student, School of CS & IT, Jain(Deemed-to-be-University), Bengaluru, India

Professor, School of CS & IT, Jain(Deemed-to-be University), Bengaluru, India

ABSTRACT: Without significant automation, humans are unable to manage the volume of data and the complexity of procedures required to safeguard cyberspace. Creating software and systems with typical fixed implementations (hardwired decision-making logic) that successfully prevent security threats is difficult. This problem can be solved with machine simplicity and AI learning approaches. This study assesses whether strengthening defensive mechanisms can improve cybersecurity capabilities and offers a brief summary of artificial intelligence (AI) applications of various cybersecurity using artificial technologies. We can determine that there are currently useful applications by looking at the most recent cybersecurity software that makes use of artificial intelligence. Neural networks are their primary tool for protecting the periphery and other cybersecurity domains. Nevertheless, it was evident that some cybersecurity problems would require the application of artificial intelligence technology. For instance, thorough information is needed for strategic decision-making, and logical decision support is one of the unmet cybersecurity needs.

I. INTRODUCTION

The complexity of malware and cyber-arms has increased dramatically in the last two years, making it clear that only intelligent technology can provide defense against advanced cyber-devices. The situation that follows "On January 15, 2009, Conficker corrupted the French Navy's computer network, Ultramar." After that, the air bases were unable to update their flight plans, so aircraft at different airbases were forced to land, and the service was placed under quarantine. Some of its important computers and gadgets have been contaminated, according to confirmation from the UK Defense Ministry. The malware has spread to government agencies, Navy Star / N * desk divisions, and hospitals in Sheffield. Over 800 machines have been verified to be infected. The Federal Republic of Germany's unified military forces, the Bundeswehr, revealed in a report dated February 2, 2009, that more than a hundred of their devices had been compromised. The Greater Manchester Police Information Network initiated a three-day preemptive disengagement of the Police Central Database in January 2010. Workers have to get in touch with specific authorities to conduct routine searches of both people and cars. Network Centric Warfare (NCW) makes cyber incidents especially dangerous, and changes to cyber defense are desperately needed. Artificial intelligence approaches and knowledge-based instruments would be essential in new offensive strategies such as dynamically establishing secure boundaries and comprehensive crisis management, as well as completely automated responses to network intrusions.

Why has there been a sharp rise in the use of smartphone apps in cyberwarfare? You will see the following reaction if you look closely at the cyber room. Artificial intelligence is first and foremost required to react swiftly to events on the Internet. A vast volume of data needs to be managed quickly in order to interpret, evaluate, and make the appropriate judgments on cyberspace activities. Before substantial technology, individuals cannot succeed in the volume of data to be used at the speed of operations. However, it is difficult to develop robots with conventional, rigid algorithms (hardwired decision-making logic) that can effectively defend against online dangers, given the ongoing emergence of new challenges. This is where intelligent automation technology is discussed.

This paper's last section discusses the scientific and technological fields that use artificial intelligence. The third chapter will examine the artificial intelligence (AI) techniques that have been proven to be effective in cyber defense. The fourth section presents new smart devices and examines the possibilities.

II. RESEARCH METHODOLOGY

We used the IEEE Xplore, Web of Science, ACM Digital Library, and Scopus databases to obtain a thorough grasp of the\ relationship between cybersecurity and AI. We also conducted searches using Google Scholar. A list of phrases that matched the topics was used to search these databases. The writers optimized a large number of search engine keywords to get maximum coverage, which improved the quality and precision of our search results.

The collected findings were filtered in the subsequent stage. We restricted our search to articles that had been published within the last four years, as the aim of this study is to showcase the most recent advancements in cybersecurity artificial intelligence. The findings were then classified according to the quantity of certifications. Additionally, papers with more than five citations were chosen. Conversely, recently published research articles with less than five references or citations and original methodologies or approaches were also chosen. After that, the following resources were approved since they satisfied [6]:

- Articles whose titles relate to topics that are not included in this research report.
- Patent documents, books, citations, technical reports.
- Articles that weren't released in English.

In order to narrow down the relevant data, we looked at the conclusions in addition to the abstracts in the third phase. This stage aided the writers in determining whether the private documents linked the subject to identify the intersection of cybersecurity and AI. Consequently, the studies that best fulfilled our goal and contained the most pertinent data were selected. To identify the gaps, a thorough assessment of the literature was the methodology used. By combining the effects of several fields, AI application in the security sector, techniques used, and techniques proposed, this study closes the gap. It is employed to create a general framework for next studies in this particular field.

AI in depth

This topic of study is relatively new, while computer systems, also known as first system intelligence, have existed for almost as long as artificial intelligence (AI). Early on in the history of artificial intelligence, devices that were meant to surpass human intelligence, such as robots, software, and structures, were viewed as "on the horizon." The problem is that the time frame gets longer as time goes on. For instance, we witnessed a range of machines master chess and resolve theoretically challenging problems. When computers were first invented, chess was considered an intellectual test. Even though electronic chess was growing in popularity in the 1970s, it was nearly impossible to create a system that could beat the world champion. However, this happened faster than expected. Three things explain this: the emergence of strong search engines, coupled with an increase in processing power. In addition to board games like chess, it can be used in a variety of software applications and contains a well-organized skill set that includes every conceivable aspect of chess knowledge (see Check section below). Since the chess problem was an abstract issue for the so-called small AI, it was successfully resolved. An other instance would be the translation of a certain AI from one dialect to another.

The 1960s have been predicted to tackle the problem of natural language processing early on, particularly in the wake of N. Chomski's computational linguistics research. Though some innovative programs, like Google's AI linguistics, showed early promise, it hasn't happened yet. This includes artificial intelligence becoming extremely knowledgeable about every facet of human activity and developing the ability to handle it. In general, artificial intelligence (AI) can be understood as a component of intellect and, more broadly, as the development of intelligent devices. AI is a technology that provides a way to solve complex problems that cannot be solved by, say, performing well or making wise decisions because of high levels of intelligence. In this article, we apply the right line, propose the application of particular AI methods in cyber defense issues and respond to the latest Artificial intelligence as illustrated in(*IOS Press*, n.d.).

1. The Role of AI in Cyber Security

1.1 AI the future of cybersecurity?

Businesses in both the public and private sectors have already embraced AI projects, with many federal departments also adopting the technology, as noted by the White House. The reason for this widespread acceptance lies in AI's capability to thoroughly analyze unstructured data, statistics, speech patterns, and words, as well as to skim through standardized data, thereby saving significant time and money. Furthermore, AI has the potential to protect both tax revenue and national secrets. However, there are still gaps in security. Hackers are constantly searching for security vulnerabilities that may not have been previously identified, and it can take years for a corporation to discover a data breach, by which time the crucial data and the hacker have disappeared. In contrast, AI can continuously monitor data and detect behavioral anomalies that could indicate a security threat, such as changes in login patterns or password resets. AI can also identify minute clues that a hacker group may have overlooked and neutralize them. However, as Varughese pointed out, anything can be misused, and human hackers will continue to probe for vulnerabilities in any system, including AI. Developers will need to implement new security protocols as cybercriminals adapt to AI systems. While the game of cat and mouse between cybersecurity experts and hackers will never end, AI can be a valuable ally in the ongoing effort to protect data. For example, Google introduced a visual data learning method for its Tensor Flow machine learning platform, integrating an open-source framework called Neural Structured Learning (NSL) on March 9, 2019. NSL is designed for both non-experts and experienced machine learning specialists and can project data from interactive databases, such as medical reports or information graphs, and perform natural language processing (NLP) in addition to rendering machine vision models."The use of organized signals during training enables developers to deliver better predictive performance, particularly if the volume of data points is fairly limited," Tensor Flow programmers wrote in a blog post today. Furthermore, structured-signal tests the ideas behind stronger models. These methods have been widely used to improve the model's performance in Google, such as learning semantic implanting of photos [14]. NSL may produce representations that use visual cues to regularize during development, whether they are monitored, semi-supervised, or unsupervised, using frequently less than ten code lines. The original system also comes with features to help developers create minimally coded APIs for vector quantization applications and organize data.

In April, Google Cloud introduced new ordered data strategies beyond AutoML Tables, such as linked sheets in BigQuery. Google AI, formerly known as Google Research, also made SM3, a compiler for large-scale speech recognition models like Google's BERT, available to the public, alongside OpenAI's GPT-2 [15].

AI has played a significant role in the development of various technologies, such as Google's search app, Facebook's facial recognition systems, and speech recognition applications like Siri. In the financial sector, AI is frequently utilized by payment card manufacturers to assist investment banks in preventing reported fraud amounting to trillions of dollars. However, the application of AI in information security is a topic of concern.

Does artificial intelligence offer advantages or disadvantages for business digital security? While modern information management architecture aids security experts in evaluating, investigating, and understanding cybercrime, it also strengthens the digital management techniques used by businesses to combat cybercrime and maintain operational and customer security. However, implementing artificial intelligence may require significant resources, which may not be feasible in all circumstances. In fact, AI could potentially be a powerful tool in the hands of hackers who leverage technology to enhance and intensify their attacks.

The discussion around artificial intelligence and information security may not have been particularly engaging in the past, as the focus of recent cyber safety developments has been on information. However, given that computers can perform tasks much faster than humans and process information in milliseconds, evaluating data through AI seems like a logical approach.

AI is gaining attention from the computer security community and is rapidly evolving. We will explore advancements in AI security technology and their impact on businesses, consumers, and cybercriminals. Let's address the issue: why are automated information protection protocols linked to higher levels of internet security?

If your company is expanding, you likely have multiple security layers in place, including border, network, edge, device, and computer storage security. For instance, in addition to network security solutions that monitor and authorize connected devices while blocking unauthorized ones, you may have hardware or software firewalls in place. If hackers manage to bypass these security measures, they must then navigate through harmful software and antivirus programs before encountering IDS/IPS systems.

However, what happens if cybercrime manages to bypass certain defenses? If your primary source of information security relies on human-based monitoring capabilities, you risk being vulnerable. Cybercrime doesn't adhere to a set schedule or correlate with your vulnerability to cyberdefenses. Therefore, you must be able to identify, locate, and respond to threats quickly, every day of the year. IT organizations should be capable and prepared to respond promptly, regardless of employee absences, holidays, or regular business hours.

1.2 What AI executives think the use of AI in information security?

In addition to their research paper titled "Reinventing Cyber Protection with AI," which underscores the importance of leveraging AI to bolster cybersecurity defenses for organizations, the Capgemini Research Institute examined information protection. This was prompted, in part, by feedback from 850 CEOs across ten different countries who participated in the study, indicating that AI-enabled solutions are imperative as hackers are already utilizing them for cyberattacks. These executives, who are leaders in IT operations, IT information management, and data security, highlighted several key points in the report:

- 75% of research participants stated that artificial intelligence (AI) enables their company to respond to breaches more swiftly.
- 69% of respondents believe that artificial intelligence is essential for businesses.
- As networks become increasingly larger and more intricate, AI will significantly bolster the enterprise's security defenses. In essence, the ever-expanding complexity of interconnected networks surpasses human capabilities. Acknowledging this is prudent; there is no need for alarm. However, it raises a crucial question: What measures are you implementing to safeguard the confidentiality of private data and customer information within your company?

1.3 Artificial intelligence technology: How do you add AI to your defence?

Integrating artificial intelligence technology seamlessly into existing information protection networks is a process that cannot be hurried. As anticipated, the preparation, training, and setup required to fully capitalize on the benefits for personnel and programs are time-consuming [20]. In a Forbes article, Naveen Joshi, the founder and CEO of Allerin, outlines various ways in which AI systems can ensure the long-term viability of cybersecurity operations. These attributes include:

- Developing accurate biometric password-based login methods
- Predictive analysis to detect risks and suspicious activities
- Improving comprehension and reasoning through natural voice recognition
- Establishing connection and identity through prerequisites

Once AI has been integrated into your information protection systems, your IT management team and information intelligence specialists will need to become proficient in using it, which necessitates preparation and time. It is crucial to ensure that the human element of the organization is not neglected. Many major players in the business sector are now integrating AI into their offerings. Here are some examples of companies that are currently using AI cybersecurity technologies: CrowdStrike, Palo Alto Networks, Check Point, Fortinet, LogRhythm, FireEye, Sophos, Symantec, and others [21].

While artificial intelligence offers numerous benefits for information security, there are also risks to consider. Implementing AI in information defense often requires more time and money than traditional, non-AI computer protection methods, which is one of the major challenges. This is partly due to the costly nature of information protection technologies built on AI frameworks. Consequently, many enterprises, especially small and medium-sized ones, have historically found them unaffordable. However, new security-as-a-service (SaaS) technologies have emerged that increase the economic viability of AI cyber defense solutions for enterprises. In reality, it is much easier to choose effective information defense strategies than to deal with the fines, delays, and other costs associated with successful but violent cyberattacks.

Addressing the vulnerabilities AI cybersecurity tools cause

Physical protection is facing additional difficulties as a result of the use of AI in information defense. While it's crucial to deploy AI technology to identify and neutralize malware threats, hackers may also employ these tools to launch progressive behavior attacks. In part, this is due to the fact that, as the costs of developing and implementing these advancements decrease, access to sophisticated AI technologies beyond machine learning methodologies is increasing [22]. This guarantees that hackers can create increasingly complex and effective malicious programs faster and for less money. The combination of factors makes one vulnerable to misuse by cybercriminals.

1.4 Adversarial AI: how hackers can misuse AI against various organizations

Information security faces a threat from artificial intelligence (AI) due to adversarial AI, a term used to describe the malicious application of AI. Accenture defines adversarial AI as the process that "causes machine learning algorithms to misunderstand inputs into the framework and respond in a way beneficial to the intruder." This occurs when intentionally altered inputs cause neural networks in AI systems to misidentify or incorrectly represent objects [23]. Without the appropriate safeguards or measures, the implications for cybersecurity could be virtually limitless. Fortunately, cybersecurity professionals are aware of the risks posed by adversarial AI. In a post on IBM's Security Intelligence research blog, it was mentioned that they are "building protections and testing AI weaknesses with pre-emptive attack models." Furthermore, IBM's labs in Dublin are actively involved in the project and have contributed to the IBM Adversarial Robustness Toolbox (ART) to combat adversarial AI.

The articles about AI technology in cybersecurity suggest that there have been several significant breakthroughs in this field. Initially, they are used for neural network perimeter shooting [28]. However, the use of AI methods is likely the only way to effectively address more cybersecurity issues. Decision-making requires the use of comprehensive information, and one of the unresolved problems in cybersecurity is the provision of reliable decision support. In the realm of artificial intelligence, numerous approaches have been developed to tackle complex issues related to human intelligence [24]. Most of these strategies have matured to the point where specific algorithms based on them are available. Some methods are now considered so commonplace that they are not considered to be within artificial intelligence. These days, they are utilized in a few applications, such as data mining techniques, that stem from the AI learning field. It will not be feasible to attempt to include a fairly comprehensive synopsis of every practical AI method in a short overview. Furthermore, we have divided methods and structures into multiple categories, such as information gathering, artificial intelligence, expert systems, smart agents, quest, computer education, and constraint solving. Here, the aforementioned classifications are outlined together with the relevant cyber protection tactics. We exclude subjects found in particular AI applications, such as robotics, machine vision, and natural language comprehension. Despite the enormous military potential offered by robotics and machine vision, no research specifically focused on cybersecurity has been done in this field [25].

III. CHALLENGES

The ability to distinguish between short- and long-term objectives will be crucial for future AI research, development, and cybersecurity applications. Many AI techniques can be swiftly applied in cybersecurity, and more sophisticated solutions than those currently in use are needed to address pressing cybersecurity issues. So far, we have discussed these new immediate applications. It would be intriguing to see entirely new concepts for information processing for decision-making and situational management presented in the future. The subject of knowledge management in cyberwarfare is highly demanding in terms of technology. Automatic information management is the only information management solution that can provide decision-makers and leaders with the rapid situational analysis they require to remain in control at all times. In the long run, perhaps we should not rely exclusively on Narrow AI for a few more decades. It is tempting to believe that by the middle of the 20th century, artificial general intelligence (AGI) will be conceivable. The first AGI conference took place at Memphis University in 2008. Established in 2000, the Singularity Institute for Artificial Intelligence (SIAI) alerts scientists to the potential for ever-faster advancements in artificial intelligence. This could lead to the Singularity, defined as "the technological development of intellect that is smarter than an individual." Future directions are often stated in terms of numerous advancements. Right now, artificial intelligence is the most talked-about, but many other advancements make it possible to build intelligent intelligence as long as they reach a certain level of complexity.

IV. CONCLUSION

In a world where hostile intelligence and cyber threats are growing exponentially, advanced cybersecurity solutions must be given top priority. Experience with DDoS avoidance has shown that, with the right tactics, security against extensive attacks can be achieved with relatively few resources. According to reviews of published articles, the study on artificial neural networks provides the most broadly relevant AI insights for cybersecurity. Although neural network applications for cybersecurity are still being developed, they have not proven to be the best solutions in many fields where sophisticated cyber-security measures are still desperately needed, such as decision support, scenario comprehension, and information control. The most interesting part of this scenario is expert machine development.

It is difficult to predict how fast general artificial intelligence will advance, but it is likely that criminals will use whatever new AI technologies become available. This is not immediately obvious. Furthermore, the cybersecurity capabilities of systems would be significantly improved by the most current technical developments in information management, interpretation, and understanding—particularly in the area of computer learning.

REFERENCES

[1] *Use of Artificial Intelligence Techniques / Applications in Cyber Defense*. (n.d.). Retrieved 14 August, 2020, from https://www.researchgate.net/publication/333477899_Use_of_Artificial_Intelligence_Techniques_Applications_in_Cyber_Defense.

[2] Ahmad, I., Abdullah, A. B., & Alghamdi, A. S. (2009). Application of artificial neural network in the detection of DOS attacks. *SIN'09 - Proceedings of the 2nd International Conference on Security of Information and Networks*, 229–234. https://doi.org/10.1145/1626195.1626252

[3] Bai, J., Wu, Y., Wang, G., Yang, S. X., & Qiu, W. (2006). A novel intrusion detection model based on multi-layer self-organizing maps and principal component analysis. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *3973 LNCS*, 255–260. https://doi.org/10.1007/11760191_37

[4] Bitter, C., North, J., Elizondo, D. A., & Watson, T. (2012). An introduction to the use of neural networks for network intrusion detection. *Studies in Computational Intelligence*, *394*, 5–24. https://doi.org/10.1007/978-3-642-25237-2_2.

[5] Carrillo, F. A. G. (2012). ¿Can Technology Replace the Teacher in the Pedagogical Relationship with the Student? *Procedia - Social and Behavioral Sciences*, *46*, 5646–5655. https://doi.org/10.1016/j.sbspro.2012.06.490.

[6] Chang, R. I., Lai, L. Bin, & Kouh, J. S. (2009). Detecting network intrusions using signal processing with query-based sampling Filter. *Eurasip Journal on Advances in Signal Processing*, *2009*. https://doi.org/10.1155/2009/735283

[7] Chatzigiannakis, V., Androulidakis, G., & Maglaris, B. (2004). A Distributed Intrusion Detection Prototype using Security Agents. *HP OpenView University Association*, *June 2014*.

[8] Chmielewski, M., Wilkos, M., & Wilkos, K. (2010). Building a multiagent environment for military decision support tools with semantic services. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6070 LNAI*(PART 1), 173–182. https://doi.org/10.1007/978-3-642-13480- 7_19.

[9] Corral, G., Llull, U. R., Herrera, A. F., Management, H., Ignasi, S., & Llull, U. R. (2007). *Innovations in*

Hybrid Intelligent Systems {--} Proceedings of the 2nd International Workshop on Hybrid Artificial Intelligence Systems (HAIS'07). 44/2008(June 2014). https://doi.org/10.1007/978-3-540-74972-1.

[10] Feyereisl, J., & Aickelin, U. (2009). *S Elf -O Rganising M Aps*. *August*, 1–30.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details