Title: The utilization of artificial intelligence in the process of intercepting rocket projectiles

Marcin Krysiak
Rzeszow University of Technology
Poland
163614@stud.prz.edu.pl

Filip Kubik
Rzeszow University of Technology
Poland
163616@stud.prz.edu.pl

Table of contents

1. Introduction

The year 2023 brought a lot of uncertainty to generations previously unfamiliar with war. The continuation of the conflict in Ukraine, which began in early 2022, and the latest events in the Middle East, raise concerns about the escalation of these conflicts on a larger scale. The threat of nuclear weapon deployment or usage by some countries has prompted a reassessment of the defense readiness of European nations. The citizens in NATO member states exert pressure on their governments to ensure adequate security within their territories. All these events have led to a focus on the development of the military industry in these countries.

The current year is also a period of intense development in computer technology, especially artificial intelligence (AI). Newly emerging platforms, chatbots, and applications have quickly gained popularity due to their ability to accelerate creative processes, such as generating a table of contents for a research article. It is well-known that computer calculations are mostly much faster, more efficient, and more precise than those performed by humans. In many engineering aspects, control systems, and devices computers can flawlessly maintain specified operating parameters. Artificial Intelligence can combine the high reliability of electronic devices with human decision-making capability.

In current missile defense systems, the usage of computers to assist their operation is common. One of the most well-known systems of this kind is the Iron Dome (1), used in the ongoing conflict in Israel. It is designed to intercept and destroy missiles, artillery, and mortar projectiles, as well as drones. A system is used, among others, by the United States Navy – the RIM-161 Standard Missile 3 (2). This system is also effective against satellites in lower Earth orbit. One of the most interesting pieces of software is the AIP Palantir (Artificial Intelligence Platform) used by the U.S. military, which supports comprehensive management of military actions. However, all these solutions suffer from a lack an autonomous decision-making system.

2. General description and goals of the system

The creation of a self-contained decision-making system based on previously analyzed data by computer can significantly contribute to more efficient operations in threatening situations. The proposed solution consists of the following segments:

- Target Analysis and Detection: Analyzing radar and satellite data to detect and classify the type of weaponry used and to determine military importance, priority of attack, and weapons.
- Tracking and Trajectory Prediction: Tracking and predicting the projectile's position over time, adjusting the flight trajectory based on atmospheric conditions.
- Risk Management: Assessing the risk associated with the enemy's weaponry and determining the optimal interception point for the projectile (regarding to the specificity of a critical infrastructure).

- Decision Making: Making decisions about automated actions or creating an appropriate action plan manually if required.
- Self-Improvement: Analyzing the accuracy of previously made decisions, making system improvements, and building a database of enemy capabilities.

The concept mentioned above focuses solely on the data analysis and decision-making aspect, but it indeed requires an executive component. The executing element is considered weaponry used in the military industry that directly responds to system commands. Various types of missile defense systems can be distinguished, such as short-range, medium-range, or long-range missiles. Furthermore, the strategic placement of this weaponry is crucial, considering their respective ranges, to ensure that each station is within the coverage of another, thereby providing self-defense capabilities. The schematic of the system concept is presented below on Figure 1:

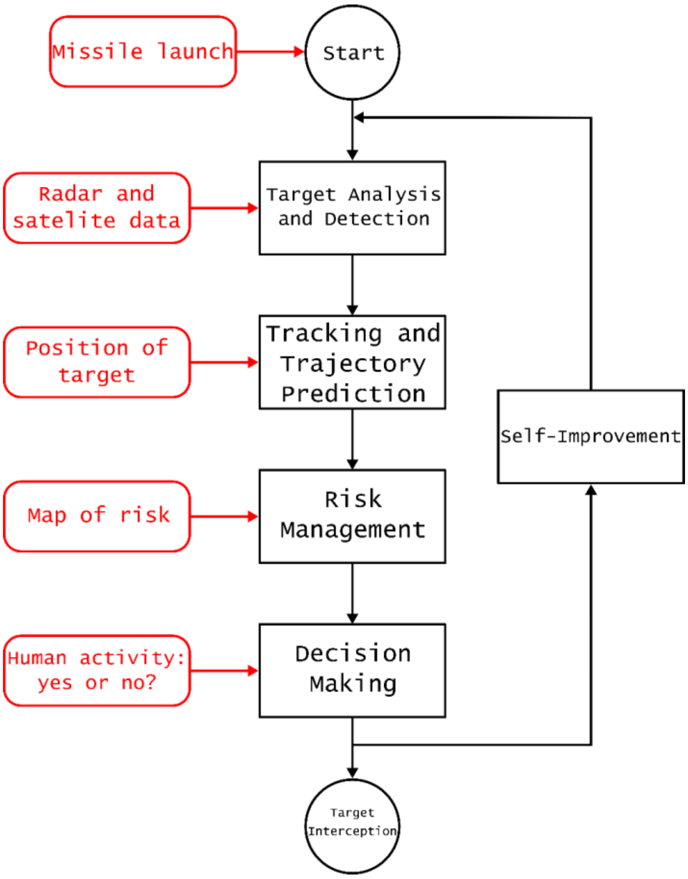

Figure 1: Diagram of proposed anti-missile system based on Artificial Intelligence

3. Target Analysis and Detection

The first task of the segment will be to analyze data obtained from radars, drones, and satellites. Radar systems are a rapidly advancing field, and an interesting aspect of it is the detection of anomalies based on infrared. It is known that a flying rocket leaves a trail of heat emitted by its jet engine, which can, in turn, be detected through infrared radiation analysis (Figure 2). Data acquired from such radar can allow for the determination of the object's speed and direction of movement. Additionally, real-time satellite images, and images from drones monitoring the area will be subjected to analysis. The data will be compared with those in the reference database to determine the most likely type of weaponry used.

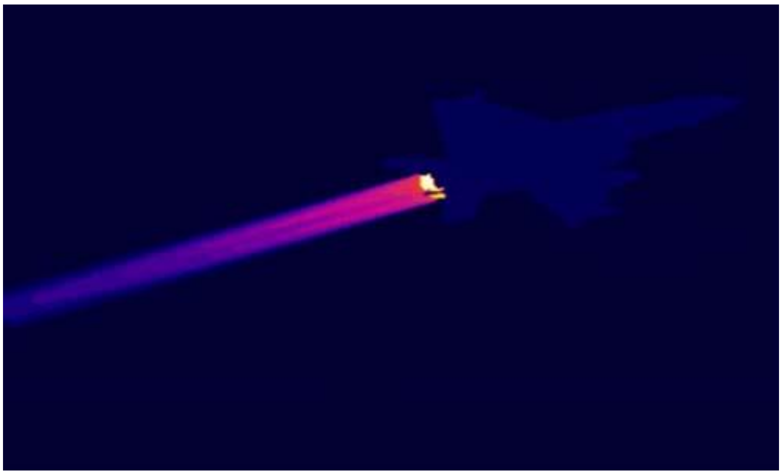

Figure 2: Heat trace behind a jet aircraft seen in infrared light. (3)

Any detection of potential threats should be promptly relayed to the person in control of the system. This is especially important in cases where the system is unable to classify the enemy's weaponry.

Multi-class pattern classification finds diverse applications such as text document categorization, speech recognition, and object recognition. Implementing neural networks for multi-class pattern classification is a non-trivial extension compared to two-class neural networks. The challenge lies in creating a system that effectively maps input features to an output space encompassing more than two pattern classes. This type of pattern recognition is integral in various fields like handwritten digit recognition, object classification, speech tagging and recognition, bioinformatics, text categorization, and information retrieval. Neural networks are typically trained separately, utilizing specific subsets of a provided training dataset. To generate the ultimate system output, a decision module is commonly employed to amalgamate the outcomes of the individual neural networks. The modeling scheme dictates the precise value and training methodology for this integration process (4).

4. Tracking and Trajectory Prediction

After detecting and classifying the threat in the form of a missile, drones will be deployed to track the weapon. This will assist in providing continuous data on the current position of the projectile. This data will be transmitted to computers whose task is to calculate the missile's position as a function of time.

Utilizing machine learning for categorizing and interpreting tracking output is a powerful technique for analyzing and reconstructing recorded data. Given the absence of precise models that establish relationships between the available variables and the ultimate outcome, employing the machine learning approach can substantially enhance the system's efficiency (5).

The algorithm for predicting the projectile's flight trajectory will be created in the form of Artificial Neural Networks with a multi-layer perceptron architecture. Such a network should be trained based on extensive training data to enable it to make accurate future predictions. It will be necessary for the algorithm to receive discrete data inputs of position over time $(x(t), y(t),\ z(t))$ and a reference time. The flight velocity will be determined as the derivative of position over time. Additionally, to enhance the accuracy of calculations, weather data will be required, including wind speed and direction. After performing the calculations, the neural network will provide the following output data:

- Projectile velocity
- Equation of the flight trajectory
- Area of probable impact of the projectile (taking into account the spread of energy)
- Time of arrival at the target

Simultaneously, the distribution of calculation and measurement errors should be analyzed based on a Gaussian process which is a stochastic process (a collection of random variables indexed by time or space) in probability theory and statistics in which every finite collection of those random variables has a multivariate normal distribution, i.e. every finite linear combination of them has a normal distribution. The Gaussian process model must be trained to represent the dependent relationship between the learning and target variables. It is worth remembering that the integral initial value, ballistic parameters, and integral time all have an impact on the numerical method's prediction of ballistic missile trajectory, and the expected error is the difference between the predicted and actual ballistic missile states. As a result, the integral initial value, the ballistic parameters, the integral time, and the true state at the forecast time are the four key factors impacting the target variable (Figure 3). However, the testing samples' actual Ballistic Missile status is never available (6).

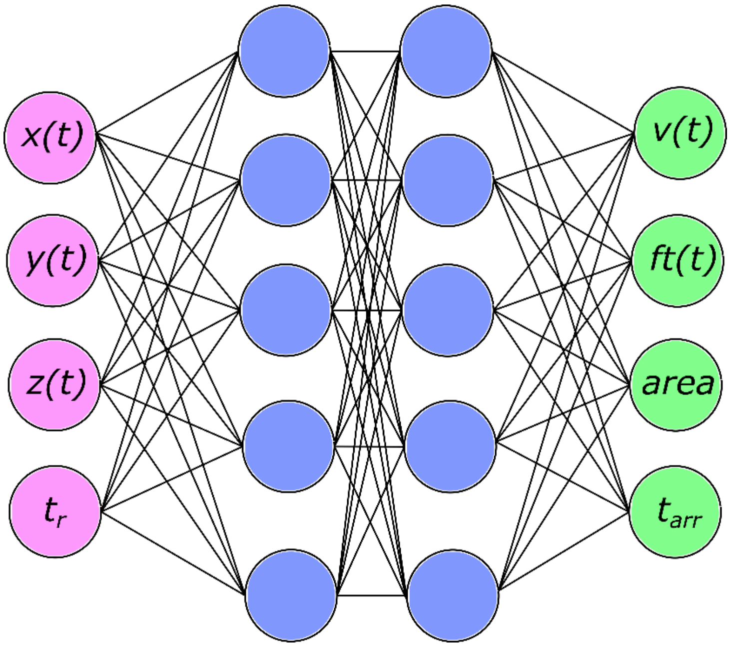

Figure 3: Proposed multilayer perceptron

5. Risk Management

Risk is an inherent aspect of every military operation. The effectiveness of the operational leader depends on achieving the right equilibrium between the risk essential for bold and decisive actions crucial for victory in combat and the lowest possible risk needed to fulfill the given mission (7). Risk analysis is an incredibly complex and extensive field in the modern world. It provides the opportunity to decrease the risk of making incorrect decisions. To optimize this process properly, several influencing factors need to be analyzed:

- Political factors,
- Economic factors,
- Social factors.

Political factors encompass all the relationships between conflicting or directly related states. Accidentally shooting down an ally's missile heading towards an enemy unit can have significant consequences. Additionally, shooting down a missile over the territory of a non-involved state can significantly worsen relations.

Economic factors pertain to issues related to the financing of military operations. Every military action incurs costs. Sometimes, the cost of an action is significantly higher than the achieved results. For example, one Russian Iskander missile used in the conflict in Ukraine costs about $3 million.

Social factors encompass all issues related to citizens and civilians. Areas with higher population densities should be better protected to minimize potential casualties. In practice, this means that such a system will attempt to intercept missiles over sparsely populated regions, like forests, fields, and less populated areas. Ethical dilemmas related to such choices are the subject of many discussions in the scientific community. Population data should be presented in the form of a population density map for easier analysis or critical infrastructure in charge of preserving the functioning of society and the defense system.

Collecting data related to each of these factors allows for the creation of a risk grid. It can be presented as the division of a given area into elementary areas, each of which would have a carefully chosen risk coefficient, represented by a certain gain value. The signal would be multiplied by the reciprocal of such gain.

0,2	0,2	0,3	0,5	0,5	0,6	0,6	0,4
0,4	0,5	0,7	0,9	0,9	0,7	0,6	0,4
0,2	0,3	0,5	0,9	0,9	0,6	0,3	0,3
0,2	0,2	0,3	0,3	0,4	0,3	0,3	0,3

Figure 4: Map of risk of certain area with signal amplifications

As seen in Figure 4, the area with a risk coefficient of 0.9 (light red color) will represent a location with a high population density, where potential civilian casualties would be significant, or possibility of high impact on society and infrastructure. Additionally, there is an area with a risk coefficient of 0.2 (light green color), which could be associated with a region of low population density and less or no significant critical infrastructure presence.

6. Decision Making

There exist various methods for decision-making, including analytical approaches and recognition-based approaches, and it's essential to comprehend the strengths and limitations of both to enhance the quality of military decision-making. It is imperative that designers of decision systems acknowledge and respect the expertise of skilled operators and take measures to ensure that their systems and interfaces do not undermine or compromise this expertise (8).

Decision-making is a key and revolutionary part of the proposed system. Previous solutions were only responsible for providing data to a monitoring system. The decision-making algorithm could be implemented using artificial intelligence (AI), which would receive all the data from the mentioned parts of the system. For such a solution, it is necessary to introduce training examples in the form of situations and decisions made by a human. A larger database allows for quicker and more accurate learning by AI of the given process. Considering all the aspects mentioned, the system would determine the most appropriate scenario in each situation, specifying the time and place for intercepting the enemy projectile. Furthermore, it would suggest the type of weaponry suitable for the task and the station from which the launch should take place. Additionally, the system would control the missile via a radio link, so that in case of a sudden change in the enemy projectile's trajectory, the defensive measure would hit its target.

It's crucial not to forget the irreplaceable role of humans in this process. The system should present all the gathered data to the monitoring individual and propose a solution to the given problem. In the development phase of this system, the ultimate decision would be made by a human taking responsibility for the action.

Human military decision-making is susceptible to judgment errors and cognitive biases, whether the engagement is carried out by a human or a machine. When examining cases involving the military's utilization of the Aegis Weapons System and the Patriot Missile System, it becomes evident that, even though the U.S. military has been actively utilizing narrow artificial intelligence in lethal, semi-autonomous weapon systems, employing these systems through a complete detect-to-engage sequence has been restricted to instances of self-defense (9).

7. Self-Improvement

The approach outlined above for creating the system leaves significant room for its development. Artificial intelligence learns from the data contained within the system, and with each operation, the volume of this data increases, leading to more accurate actions. The primary parameter in the feedback loop should be the success of interceptions – the system should record successful interception cases and calculate adjustments for subsequent decisions. Additionally, it should collect characteristic elements of the enemy's weaponry in a database, which will facilitate further detection and classification of projectiles. This will allow for the creation of an enemy arsenal model. Furthermore, the frequency of threat detection will help determine the locations where the enemy's weapons are stationed and the areas most at risk of their attack.

Human decision-making is an integral part of the process, but based on human choices, artificial intelligence can learn to make similar actions depending on the given scenario. Artificial intelligence is a tool that, over time, minimizes its errors. Improving AI performance is a process that requires constant care, research, and experimentation, but it can lead to a significant improvement in the quality and effectiveness of AI-based systems. The system should remain under human supervision, but once it reaches a sufficiently low probability of making mistakes, it could operate autonomously.

8. Conclusion

Artificial intelligence is considered by many to be the future of today's technology. However, in the modern world, there is still a lack of many legal regulations aimed at systematizing its use. These regulations would clarify the purpose, limitations, and responsible parties of operating such systems. It's important not to forget the societal attitude towards such technology and the societal response to the information that long-range weapon control systems are operated by computers.

Artificial intelligence-based systems have the capability to rapidly analyze data from multiple sources and fuse them. They can gather information from different databases, meters, or sensors measuring various physical parameters, compare them, and arrive at appropriate conclusions. Furthermore, machine learning enables defense systems to adapt to changing conditions, identifying patterns in real-time. They are also responsible for predicting projectile trajectories, aiding in precise target calculation and attack timing, which increases the chances of defense against an adversary's attack. Over time, with increasing training data, AI can effectively adjust its strategy and tactics based on the evolving situation. For this reason, a control system can effectively counter adversary projectiles with changing flight trajectories and speeds. Autonomous systems based on artificial neural networks can operate directly and make decisions independently, responding quickly to threats, which is crucial in the case of unforeseen attacks.

The solution involving the creation of a risk grid allows for the selection of the optimal intercept location for a projectile. This process enables the minimization of civilian casualties on the defending side. It is also a very fast and efficient tool for analysis, transparent and straightforward for computer software to handle - such a grid can be represented in a computer's memory as a vector. Additionally, this approach can prevent accidental interception of a rocket over weapon depots or explosive materials.

However, it is essential not to forget about securing the created system. Securing the data flow network in the context of wireless communication systems is a crucial element in maintaining the integrity, accuracy, and availability of information data. The implementation of effective authentication mechanisms is required to ensure that only authorized individuals or systems have access to the data. Data encryption during storage and transmission is a significant means of protection against unauthorized access. Constant development and adaptation of security strategies to the evolving cybersecurity landscape are crucial for effectively safeguarding data in the AI environment.

In the era of universal access to electricity and the Internet, such a system would have versatile applications in any location on Earth. The widespread accessibility of technology raises security concerns due to reduced costs and ease of access. There is a need for more comprehensive regulation to safeguard society from technologically advanced malicious actors who could potentially develop highly dangerous equipment and solutions using readily available knowledge. Although Chemical, Biological, Radiological, and nuclear technologies are typically subject to strict regulations, these regulations might prove insufficient (10).

References

1. [Online] https://en.wikipedia.org/wiki/Iron_Dome (accessed 27.10.2023).

2. [Online] https://en.wikipedia.org/wiki/RIM-161_Standard_Missile_3 (accessed 27.10.2023).

3. [Online] http://www.thermofluids.co.uk/femview.php (accessed 27.10.2023).

4. Guobin, Ou and Yi Lu, Murphey. Multi-class pattern classification using neural networks. 2007 (ISSN: 0031-3203).

5. García, Jesus, et al. Trajectory classification based on machine-learning techniques over tracking data. 2006. (ISBN: 1-4244-0953-5).

6. XU, Linfeng, et al. Trajectory prediction of ballistic missiles using. *Chinese Journal of Aeronautics.* 2021.

7. Tanner, James. Operational Risk Management at the Operational Level of War. 1997.

8. Klein, Gary. Strategies of Decision Making. 1989.

9. Montgomery, Christi. AI, Autonomy, and Military Decision Making with Lethal Consequences. 2019.

10. SZABADFÖLDI, István. Artificial Intelligence in Military Application – Opportunities and Challenges. 2021.