v. 4, n. 6, 2024

Journal of
Engineering
Research

THE USE OF ARTIFICIAL INTELLIGENCE AS A NATIONAL DEFENSE STRATEGY

João Pedro Santos Nanni
Graduating of the Quartermaster Officer Training Course (CFOInt) at the Air Force Academy (AFA), currently studying third grade
Air Force Academy
Pirassununga - São Paulo
http://lattes.cnpq.br/2658031034262091

Gabriel Almeida de Azevedo
Graduating from AFA's CFOInt, studying third grade
Air Force Academy
Pirassununga - São Paulo
This student does not have a Lattes Curriculum

Daniel Torres Farias Alencar
Graduating from AFA's CFOInt, studying third grade
Air Force Academy
Pirassununga - São Paulo
This student does not have a Lattes Curriculum

Koffi Arnold Apolinarie Kini
Graduating from the Aviation Officer Training Course (CFOAv) da AFA, cursando a terceira série
Air Force Academy
Pirassununga - São Paulo
This student does not have a Lattes Curriculum

DOI: https://doi.org/10.22533/at.ed.317462423028

Homero Henrique Nepomuceno Bortolussi
Graduating from AFA's CFOInt, studying second grade
Air Force Academy
Pirassununga - São Paulo
This student does not have a Lattes Curriculum

Guilherme Augusto Spiegel Gualazzi
Professor of Information Technologies, Information Systems and Cybernetics at AFA
Air Force Academy
Pirassununga - São Paulo
http://lattes.cnpq.br/0634103496258984

Abstract: Considering the increasingly rapid development of Artificial Intelligence technology, its influence on National Defense Capabilities has become evident. In this context, the possibility of using an intelligent system to supply these capabilities is envisaged. With the advancement of technology and artificial intelligence, a relationship was established between the learning system, known as "machine learning", and the various defense systems such as Intrusion Detection, Recognition and Characteristic Identification Systems. It is important to highlight that the sectors involved in this method constitute part of the national defense policy of their respective countries, reinforcing the relevance of a thorough analysis of their importance on the world stage. In view of this, the present work aims to carry out a comprehensive analysis of the global panorama of systems that use artificial intelligence techniques within the scope of national defense. To this end, the sample space was restricted to the study of the fifteen largest economies of 2022, analyzing scientific articles, reports from specialized institutions and widely disseminated news.

Keywords: National Defense, Artificial Intelligence (AI), Machine Learning.

INTRODUCTION

The use of Artificial Intelligence (AI) has become increasingly present in different areas of society. According to a report by Markets and Markets (2022), the AI market is projected to grow from US$86.9 billion in 2022 to US$407 billion in 2027. One of the areas that has explored its potential is National Defense, with countries such as the United States, China and Russia carrying out research on this topic (BARREIROS et al, 2021). Aiming to improve the country's security and protection, AI has been used as a strategy to assist in various activities, such as threat detection, decision-making and planning military operations.

AI does not have a formal definition that is widely accepted, since for Rich and Night (1991), conceptualizing this topic would be ephemeral as it refers to an area of computing, and thus fails to encompass a new area. For Sichman (2021), what becomes appropriate is the definition of your objectives. “The goal of AI is to develop systems to perform tasks that, at the moment, are better performed by humans than by machines, or do not have an algorithmic solution viable by conventional computing.” (RICH E NIGHT, 1991, apud SICHMAN, 2021).

According to Sichman (2021), the history of AI dates back to the 1950s, and the development of computing itself. The first milestone in this development was made in 1956, with the Darthmouth College Conference in the United States, which brought together several experts to discuss the creation of software that could simulate human intelligence.

AI has developed exponentially over the last 6 decades, becoming a technology widely present in areas such as Health, Industry and Smart Cities, such as the approaches of the Applied Research Centers promoted by the Brazilian government according to the Ministry of Science, Technology and Innovation (BRAZIL, 2021). In National Defense, AI has been used to assist in activities that require great precision and speed, such as voice, speech and facial recognition, the detection of suspicious movements in border areas and data analysis to predict possible attacks, both physical and physical. as well as cyber, as shown in the Brazilian Artificial Intelligence Strategy (BRAZIL, 2021).

Furthermore, AI has also been used to assist in decision-making and governance processes, as shown in the Brazilian Artificial Intelligence Strategy, allowing the military to access relevant information quickly and accurately. This can be particularly useful in conflict situations, where the speed and accuracy of information can make the difference between the success and failure of an operation.

However, the use of AI in National Defense also presents challenges and threats. For Dietterich and Horvitz (2015), and as taken up by Sichman (2021), there are 5 large sets of risks:

1. Software errors: all systems are subject to bugs, but these in critical systems can be accompanied by large costs and resulting deaths.

2. Cyber protection: like other computer systems and software, AI systems are vulnerable to cyber-attacks.

3. Sorcerer’s apprentice: just as in the tale of the sorcerer’s apprentice, the AI must be able to analyze the command given, not carrying out undesirable activities due to the unreasonableness of the order.

4. Shared autonomy: one of the challenges of implementing AI systems is the transition of responsibility and command between the machine and its operator.

5. Socioeconomic impacts: AI is capable of influencing all spheres of society, causing various impacts that must be understood.

One of the possible areas of activity for systems that use AI techniques is Intrusion Detection Systems in computer networks, due to the large volume of data and the need for rapid action. According to the Center for Studies, Response and Treatment of Security Incidents in Brazil (CERT.br), from 2011 to 2020, 6,685,512 incidents were reported. This reality is also constant in other countries. Additionally, the Cybersecurity and Infrastructure Security Agency (CISA) report shows that in 2020, there were more than 2000 cyber incidents that affected federal agencies, critical infrastructure, and other organizations in the United States. This information corroborates the idea that the current situation is an environment of constant conflict and threat to all institutions and nations. Therefore, this is one of the critical areas that allow the influence of AI to contribute to National Defense.

In this context, the objective of this work is to analyze the use of Artificial Intelligence applied to National Defense by several countries, highlighting those that have indicators of use of these systems, to verify their degree of importance at a global level.

After this brief introduction, the methodology used is presented and then the theoretical foundation that supports the analyses. In the third section, the main results and a brief discussion are presented. Final considerations conclude the work.

METHODOLOGY

To achieve the proposed objective, this research uses bibliographical research, at an exploratory level, as stated by Gil (2010, p.44), regarding the application of Artificial Intelligence within the scope of nations. The aim is to list evidence of the use of this applied technology as a defense tool and place it from the perspective of the National Defense Strategy. We chose to analyze the 15 largest economies in 2022, as per Annex A.

This quantity is justified to include Brazil and Mexico and consider these two Latin American countries in perspective with the other nations with higher GDP. In addition to the 15 nations, States identified as exponents in the area were included. Fundamentally, bibliographic sources were sought, according to the categories stated by Gil (2010, p.44):

A. The scientific framework of periodical publications using as keywords: National Defense, Artificial Intelligence (AI). The articles were mainly taken from platforms such as SciElo, Science Direct and Springer.

B. Commonly read books, which are characterized as publicity works, and reference books.

C. Various forms such as:

The. Incident reports, taken from platforms such as CGI.br, CISA.

B. Journalistic records, as they are understood as a source of information with a shorter time interval between the event and its publication, when compared to scientific articles. These were taken from various platforms, as mentioned in the bibliography, from the period between 2013 and 2023.

THEORETICAL FOUNDATION

The National Defense Strategy is a set of actions coordinated by the State to guarantee the protection of the territory and the population against external threats. It is made up of a set of policies, measures, plans and actions that aim to guarantee national security in several areas, such as military defense, border security, cyber security and defense against chemical, biological, radiological and nuclear threats. And through these, guarantee the objectives described in the National Defense Plan (BRASIL, 2022).

Artificial Intelligence systems are used in several nations, among the uses that are related to the competencies expected within National Defense. For the National Defense Strategy (BRASIL, 2022), the capabilities are: Protection, Prompt Response, Deterrence, Coordination and Control, Information Management, Logistics for National Defense, Strategic Mobility, Mobilization and Defense Technological Development.

Artificial Intelligence, for Allen and Chan (2017), can develop comprehensive problem-solving skills in its own algorithms, which makes it grow exponentially. (CÔRREA, 2021). For Janiesch et al. (2021) Machine Learning techniques can be summarized as systems that automatically seek to learn from significant relationships and patterns coming from examples and observations. And with advances in this technology, it is now possible to identify, in society, the rise of intelligent systems with human-like cognition.

According to Janiesch et al. (2021), Machine Learning algorithms stand out in regression, clustering and classification applications, being dependent on data sets from specific problems to be able to understand the correlations and nuances of the activity to be performed. This way, they stand out in activities such as next-best offer analysis (NBO), identification of patterns or exceptions, such as detection of fraudulent documents, recognition of emotions, behaviors, speech and image, as well as natural language processing (NLP).

According to Chen et al. (2023), ML techniques can be used in the analysis of data resulting from imaging, such as in the classification of hyperspectral images (HSIs), being able to precisely identify the terrain, with its properties, such as relief, vegetation, resources and facilities. This type of analysis provides vital data for National Defense, especially when applied in the theater of operations.

As identified in the Brazilian Artificial Intelligence Strategy (BRASIL, 2021), AI systems provide great decision assistance to the manager. This influence then directly impacts component parts of the Armed Forces, such as Command and Control activities.

Furthermore, for Leys (2018) AI can be used in Autonomous Weapon Systems (AWS), which are capable of operating or not in conjunction with humans, and when independent, can improve reaction times and the period of availability. Furthermore, in conditions of loss of communication, AWS systems, unlike remotely controlled ones, are capable of maintaining their operational capabilities in the face of different scenarios that may be encountered, this being an integral objective of the Defense Equipment Articulation Plan in the National Defense Strategy (BRAZIL, 2021).

Another application of AI in National Defense is data analysis to predict conflict situations. Through intelligence analysis, AI can identify trends and patterns that may indicate an imminent conflict situation, allowing National Defense to take preventive or early response measures. Additionally, AI can be used to monitor the activity of terrorist groups and predict terrorist attacks.

AI techniques can also be used in Intrusion Detection Systems, both related to the invasion of physical areas and cyber environments. For Saranya et al. (2020, p. 2), with the large volume and speed of data circulation, traditional data detection methods are not able to detect intruders in the fastest way. With this in mind, in order to enable the efficient identification of attacks, based on the analysis of network traffic, the Intrusion Detection System can use ML algorithms, which can be conceptualized as computer programming to optimize performance criteria using example data or past experiences, according to Alpaydin (2020). Having a model defined with some parameters, learning is the execution of software to optimize these model variables using example data or previous learning.

The use of ML Systems influences several areas, with the Brazilian Artificial Intelligence Strategy (BRASIL, 2021) mentioning the knowledge that Artificial Intelligence technology stands out in its use in Intrusion Detection Systems. As highlighted in the graph below (FIGURE 1), IDS methods, based on ML, have high accuracy, as shown in Saranya et al. (2020), being a difference between other methods.

Given the facts presented, it is worth highlighting that, in 2018, the main use of artificial intelligence was already in the area of detecting and blocking intruders, vital for National Defense, as shown in figure 1.

RESULTS AND DISCUSSION

Data from the following countries present asymmetry regarding the amount of content presented. This is due to the greater volume of data and references found from some countries, as they act more present on the international scene, which is to be expected due to their technological advancement and efforts in the area of defense. According to the Carnegie Endowment for International Peace (2019), the countries that have the greatest capacity to provide this technology are the United States and China. The report also shows the presence of other nations in the scenario. At the end, item 5.17 is presented, which combines the results presented in each country.

U.S

According to Markets and Markets (2020) report, the United States has the largest market for IDS and government agencies such as the Department of Defense (DoD) and the National Security Agency (NSA) are using ML to improve their capabilities cybernetics.

According to Obis and Macri (2022), the National Defense Authorization Act (NDAA) of 2023 emphasized the development of Artificial Intelligence, with a focus on continuing the acceleration of technology, as has already been occurring, and this development being a priority in the so-called Joint All- Domain Command-and-Control (JADC2), with the July 2022 symposium being motivated by the question of how to keep JADC2 elements state-of-the-art. The NDAA 2023 also established a 5-year implementation plan for Artificial Intelligence systems within Cyber Warfare missions. "In its fullness, this [Artificial Intelligence] will impact vulnerability management, threat hunting and boost network security." (apud. OBIS; MACRI, 2022, our translation).

The United States Cyber Command (2019) also recognizes, in the Technical Challenge Problems Guidance, as its 15th challenging problem that the USCC is interested in using ML to characterize and detect unknown malware in computer networks. Being the 17th challenging problem related to the implementation of these Artificial Intelligence systems. The Responsible Artificial Intelligence Strategy and Implementation Pathway foresees that the use of ML in detecting attacks is one of the necessary steps in the implementation plan of AI tools

According to Thornton (2022, our translation), "Dave Frederick, executive director of CYBERCOM, said that DoD has already integrated basic commercially available applications and products into its cyber defense mission." Including using it to reduce the workload of cyber analysts when identifying malware. This section elucidated by Thornton shows the United States' objective in using an IDS based on ML.

According to Gitlin (2023), the United States Air Force (USAF) has already acquired the ability to use aircraft such as a modified F-16, X-62, autonomously, having basic aircraft capabilities such as landing and takeoff. The National Artificial Intelligence Initiative foresees the investment and development of Intelligence in order to keep the United States at the forefront of the development of this technology.

CHINA

China has invested heavily in the last decade in the development of ML and artificial intelligence, cyber protection is no exception to this. Its development is mainly aimed at International Competitiveness, seen as a strategic project. According to the Carnegie Endowment for International Peace (2019),

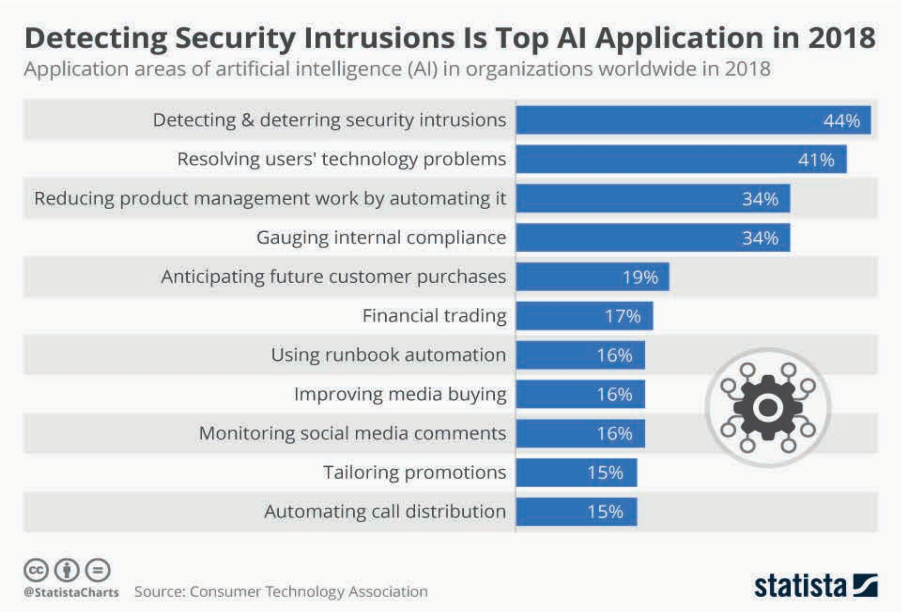

FIGURE 1: Artificial Intelligence Application Areas in 2018

Source: FELDMAN (2018). Available at: Detecting Security Intrusion is top AI Application in 2018

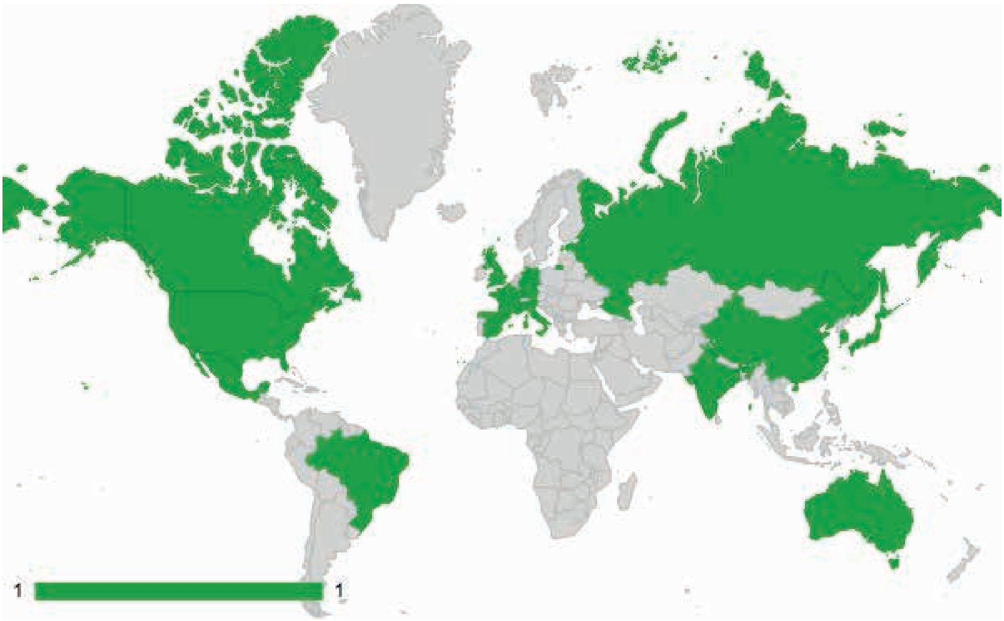

FIGURE 2: Countries with Evidence of the Application of Artificial Intelligence in 2018

Source: The authors

China is the largest carrier of AI Technologies, in addition to using technologies both from its own nation and from the United States, having both facial recognition technologies, as well as Cities and Smart Policing.

According to Roberts et al (2021), in 2017 the New Generation Artificial Intelligence Development Plan was published, which is a document that unifies and describes Chinese objectives regarding AI, for this purpose it establishes several objectives on the subject, highlighting the country's goal to become the world leader in Artificial Intelligence innovation by 2030.

The documentation highlights three areas of importance: the first is international competition, as part of providing leaps in its military capacity, mainly to face American military power using asymmetric warfare tactics, and within that term cyberwar. The second area is economic development, establishing AI as the driving force behind a new cycle of industrial transformation, although there is the possibility of it disrupting relations in the labor market. The last area is social governance, China has been facing emerging social problems due to the aging of the population, use of natural resources, etc., and to overcome them, legislation provides for the use of AI to manage public services, seeking precision and improvement. of quality of life.

JAPAN

The Japanese Government, through the National Security Strategy and its subsequent review with observations made in the Ukrainian War, defines its priorities in the medium and long term. The two main changes brought about by the review, regarding cybersecurity, are the development of an information warfare posture and the introduction of active cyber defense. The second modification gives the Japanese government the power to defend essential infrastructure, retaliate in cyberspace and neutralize attackers.

There are also several initiatives motivated by the State, which focus on promoting the development of artificial intelligence in cyber protection, including the "Cyber Security Vision" plan, which has this technology as one of its focuses.

According to Osawa (2023), Japan, with the new National Security Strategy, plans to improve the monitoring of information space and strengthen intelligence analysis. In addition to planning the implementation of an information collection and analysis system using AI to assist with battlefield awareness.

GERMANY

According to the panorama (BRAZIL, 2022b), Germany intends to consolidate itself as a reference in the AI sector, still highlighting 12 fields of action and 14 goals in the strategy. In these points listed, the role of the competence centers of the Federal Office for Information Technology Security (BSI), in German Bundesamt für Sicherheit in der Informationstechnik, is highlighted to bring together expertise and provide consultancy on information security for both AI, and through AI, in addition to the defense against attacks being assisted by AI.

The German armed forces are one of the only ones in the world to have an organizational unit dedicated to cyber defense, in English called the Cyber and Information Domain Service.

The German government has implemented several measures to increase its cyber protection capabilities, including the use of ML-based IDS. In 2020, the Federal Office for Information Technology Security (BSI), in German Bundesamt für Sicherheit in der Informationstechnik, launched a project to test the effectiveness of this technology. This initiative involved analyzing network traffic scenarios and identifying threats in real time.

There are still research institutes and companies in the country that are developing and providing cyber protection systems using this technology, such as the Fraunhofer Institute for Information Technology Security (SIT).

According to Sauer (2018), the German armed forces are already developing systems based on Artificial Intelligence technology with a focus on areas such as obtaining AWS.

UK

The Department for Digital, Culture, Media & Sport (2022) announced that the UK has implemented several measures to increase its cyber protection capabilities, including the use of ML in IDS systems. In 2020, the UK's National Cyber Security Center (NCSC) published a report on the use of AI in cyber protection. This report highlights the potential benefits of using these systems to detect and respond to cyber threats in real time.

According to Zahra (2021), the UK education sectors produce many publications on AI. In the period from 2010 to 2020, these sectors contributed 1,400 research initiatives to develop the Artificial Intelligence system.

According to the United Kingdom (2023), the country has also funded research and development groups for projects focused on AI-based IDS. One of the funders, for example, the UK Defense and Security Accelerator (DASA) provided funding for several projects in this area with IDS and IPS, including ML.

INDIA

According to SAAED (2023), established in 2022, the Defense Artificial Intelligence Council (DAIC), subordinate to the Indian ministry of defense, aims to offer guidance and encouragement for innovations that contain advanced technology, aiming to create 25 AI products for industry of defense until 2024. Another recent creation is the Military AI Project Agency (DAIPA), with more than 13 million dollars in annual budget, focusing on projects to aid the decision-making process, border security and autonomous systems, such as drones and vehicles terrestrial.

FRANCE

According to Poussielgue (2018), as a reflection of this promotion, in 2018 President Emmanuel Macron announced that the country will invest 1.5 billion euros in AI research over the next 5 years. Opened in 2022, the cybersecurity campus in Paris is a building that brings together more than 1,700 professionals in the field, with military and industrial backgrounds. It aims to be a research and training hub in the field, aiming to unify efforts for a better response to cyber-attacks.

ITALY

According to Cervini (2021), Italy's AI is inspired by the European Union's Coordinated Plan on AI. The Italian government is part of the joint effort to improve the harmony of rules proposed by the European AI regulation.

Furthermore, the Italian government, through the Ministry of Technological Innovation and Digital Transition (MITD), formulated the Artificial Intelligence Strategic Program, which aims to develop an Artificial intelligence ecosystem, increase funding for research in the area and encourage application of AI both in public administration and in the private sector.

The Artificial Intelligence Strategic Program (ITALY, 2022) defines national defense as a priority sector for the development of AI and states that the country has committed to investing in national cybersecurity, in which AI will contribute to the new generation of AI software. threat detection.

According to Bozzetti et al. (2021), the Observatory of Digital Attacks (OAD) is the only independent online survey in Italy on intentional attacks on the information technology systems of companies and public bodies and, in this country, cyber-attacks constitute a growing and serious risk.

Given this, Bozzetti et al. (2021) states that, in the OAD survey carried out in 2020, this demonstrated an improvement in digital security measures in the country, however, the most modern artificial intelligence prevention, protection and management techniques are still in the initial stage of development among interviewed.

CANADA

According to Khraisat (2019), in 2018, the CSE-CIC-IDS 2018 was generated, the most recent and realistic set of cyber data from the Canadian Establishment for Cybersecurity (CIC) to date. CIC datasets have been used around the world for intrusion detection and malware anticipation.

The main objective of this data is to orderly construct a way of dealing with the different production and long range of benchmark data sets for detecting intruders in the formation of customer profiles, which contain theoretical representations of occasions and practices seen in the system.

SOUTH KOREA

According to Kim (2022), the South Korean government is turning to AI-based systems to enhance the capabilities of the military as a defense strategy. Due to factors such as the declining birth rate, authorities are investing in defense innovation 4.0.

RUSSIA

According to Konaev (2021), Russia develops AI applied in the military environment in several approaches, including: electronic warfare, the country has been developing since 2009, with AI techniques being added to increase its effectiveness in signal classification and translation of information; unmanned systems, Russia develops unmanned vehicles for all 4 physical environments of modern combat, as an example of the S-70 Unmanned Aerial Vehicle; informational superiority and cyber warfare.

AUSTRALIA

According to Devitt et al. (2022) Australia is seeking to achieve the capability to operate AWS, including autonomous aircraft operation. The proposal to use these AI techniques also encompasses the competence of Command and Control.

SPAIN

In Spain, the National Cryptological Center (CCN) was created in 2006, tasked with protecting systems, public or private, of strategic importance from cyberattacks. It is also responsible for coordinating the use of AI for its mission, according to the CCN-CERT itself (2022).

BRAZIL

At the beginning of 2021, the Brazilian Artificial Intelligence Strategy (EBIA) was created. This document states that a National AI Strategy must aim to develop this and use it so that the scientific scenario can evolve and seek to resolve certain palpable problems in the country. To this end, an analysis would be carried out and the highest priorities defined according to their likelihood of generating benefits for the nation. According to the Carnegie Endowment for International Peace (2019), the United States uses technologies from both the United States and China, having both facial recognition technologies and Smart Cities and Policing.

MEXICO

According to Dillon (2022), Christopher Krebs, former director of the United States Cybersecurity and Infrastructure Security Agency, Mexico needs to better protect itself from cyber-attacks that could be carried out by China or Russia.

His speech is pertinent considering that the Mexican Ministry of National Defense (Sedena) and the Ministry of Infrastructure, Communications and Transport (SICT) were victims of a cyber-attack carried out by a group of activist hackers called The Guacamaya. The group infiltrated Sedena's servers and stole millions of emails and documents while unidentified hackers breached the security of 110 SICT computers and installed ransomware, according to México News Daily.

OTHER EXPONENT NATIONS

ESTONIA

According to the European Commission (2020), the Government is the most prominent in Europe in terms of internet integration, with 99% of services available online. Furthermore, between 2019 and 2021 it invested €10 million in order to implement its AI strategy. Another capability, powered by AI techniques, is the analysis of satellite imaging data, which the nation already uses as in the Ministry of Agriculture.

SUMMARY OF THE SURVEY

From the systematic literature review carried out, it was possible to identify that of the 16 countries surveyed, 16 present strong indications of considering this technology as one of the national developments focuses or are using it.

The data can be seen in Figure 2, where the countries in green are those where signs of use were found, and those in red, where the signs were low. The other countries that are outside the research are shown in gray.

It is worth noting that it is not possible to infer whether there is the use or development of technologies given the sensitivity of the information regarding defensive capacity.

According to the Brazilian Artificial Intelligence Strategy (BRASIL, 2021), "AI has also proven useful in preventing and detecting the invasion of computer networks and IT devices", a fact proven by the reports cited below. As an example, elucidated by the strategic document, the following cases were highlighted, according to Darkreading (2022), in which artificial intelligence managed to prevent cyber-attacks:

- In early 2021, a private equity firm looking to bolster its email security efforts tested an AI email security solution and detected a spoofing attack. The attackers adapted their email to mimic the company's internal HR communications. Further investigation showed that the email is part of a broader trend of targeted phishing campaigns that use fake Microsoft branding to trick employees.

- In March 2022, a South African financial services company discovered an ongoing ransomware attack attempting to encrypt its data. The first sign of compromise was a company email server making unusual HTTP connections and communicating with a malicious server. Its understanding of the business and normal behavior of this particular email server allowed the AI to identify the threatening activity.

CONCLUSION

It is worth noting that the objective of the work was not to address the stage of development that each country's program is in, with these indications being based on the use of AI methods applied in different areas of defense.

With this, it is concluded that, when analyzing the countries in this work, the importance of using AI in the area of National

Defense is verified, considering that around 100% of the nations analyzed are already, at least, giving evidence investment in this scenario. Using the aforementioned reports of blocking hostile connections by AI, the application of ML, in addition to being a practice that already has strong indications of being widespread among nations, is also a method that was able to prevent several malware attacks.

Therefore, as most of the largest nations, from an economic point of view, consider AI to be a relevant technology for National Defense and are increasingly seeking to make investments in this area, the importance of the object studied in this work can be assessed.

REFERENCES

ALLEN, G.; CHAN, T. **Artificial Intelligence and National Security**. [s.l: s.n.]. Disponível em: <https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf>.

ALSINAWI, B. **Understanding the implications cyberwarfare has on your cybersecurity strategy**. 30 jan. 2019.

BOZZETTI, M. R. A.; OLIVIERI, L.; SPOTO, F. **Cybersecurity impacts of the covid-19 pandemic in Italy.** Disponível em: <https://ceur-ws.org/Vol-2940/paper13.pdf>. Acesso em: 26 abr. 2023.

BRASIL. **Estratégia Brasileira de Inteligência Artificial**. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-documento_referencia_4-979_2021.pdf>. Acesso em: 27 abr. 2023.

BRASIL; Ministério Da Ciência, Tecnologia e Inovação. **Inteligência Artificial Centros.** Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial-centros>. Acesso em: 27 abr. 2023.

BRASIL; Ministério da Defesa. **MD31-M-07**: **doutrina militar de defesa cibernética**. [s.l: s.n.]. Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/123456789/136/1/MD31_M07.pdf>.

BRASIL; Ministério das Relações Exteriores. **Políticas Nacionais e Institutos de Inteligência Artificial**. [s.l: s.n.]. Disponível em: <https://www.gov.br/mre/pt-br/assuntos/ciencia-tecnologia-e-inovacao/PanoramaInternacionalPolticasNacionaiseInstitutosdeIntelignciaArtificialV2.pdf>. Acesso em: 15 jun. 2023.

BRASIL. Portaria nº 93. **Dispõe sobre Glossário de Segurança da Informação. Brasília, Distrito Federal: Gabinete de Segurança Institucional da Presidência da República**, set. 2019. Disponível em: http://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663. Acesso em: 20 abr. 2023.

CANCINO, B. **Cybersecurity in Mexico**. Disponível em: <https://www.lexology.com/library/detail.aspx?g=60c54f8c-7cce-4dac-89b8-79dfb217e054>. Acesso em: 25 abr. 2023.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE. **AI Global Surveillance.** Disponível em: <https://carnegieendowment.org/publications/interactive/ai-surveillance>. Acesso em: 27 abr. 2023.

CCN-CERT. **Mission and objectives**. Disponível em: <https://www.ccn-cert.cni.es/en/about-us/mission-and-objectives.html>. Acesso em: 27 abr. 2023.

CORRÊA, Françoa Taffarel Rosário. Estudo do emprego de Inteligência Artificial no contexto da Guerra Cibernética. **DATA & HERTZ**, v.2 n.2, p 19-25,2021.

CHEN, Y.-N. et al. Special Issue Review: Artificial Intelligence and Machine Learning Applications in Remote Sensing. **Remote Sensing**, v. 15, n. 3, p. 569–569, 18 jan. 2023.

DARKREADING. **5 Surprising Cyberattacks AI Stopped This Year.** Disponível em: <https://www.darkreading.com/dr-tech/5-surprising-cyberattacks-ai-stopped-this-year>. Acesso em: 27 abr. 2023.

DEVITT, S. et al. **Australia's Approach to AI Governance in Security & Defence**. [s.l: s.n.]. Disponível em: <https://arxiv.org/ftp/arxiv/papers/2112/2112.01252.pdf>.

DIETTERICH, T. G.; HORVITZ, E. J. Rise of concerns about AI. **Communications of the ACM**, v. 58, n. 10, p. 38–40, 28 set. 2015.

DIMOLFETTA, D. **2023 defense bill supports DOD adoption of more AI for cybersecurity.** Disponível em: <https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/2023-defense-bill-supports-dod-adoption-of-more-ai-for-cybersecurity-73477388>. Acesso em: 26 abr. 2023.

DILLON, K. **Cyber Specialist Issues Warning on Mexico 's Vulnerable Cybersecurity** - Pulse News Mexico. Disponível em: <https://pulsenewsmexico.com/2022/10/28/cyber-specialist-issues-warning-on-mexicos-vulnerable-cybersecurity/>. Acesso em: 23 abr. 2023.

EUROPEAN COMMISSION. **Estonian public services in the age of Artificial Intelligence | Advanced Technologies for Industry**. Disponível em: <https://ati.ec.europa.eu/news/estonian-public-services-age-artificial-intelligence>. Acesso em: 24 abr. 2023.

FELDMAN, S. **Infographic**: Detecting Security Intrusions Is Top AI Application in 2018. Disponível em: <https://www.statista.com/chart/17630/artificial-intelligence-use-in-business/>. Acesso em: 25 abr. 2023.

FELDSTEIN, S. **The Global Expansion of AI Surveillance.** Disponível em: <https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>. Acesso em: 26 abr. 2023.

FOR, Department. **New ten-year plan to make the UK a global AI superpower**. GOV.UK. Disponível em: <https://www.gov.uk/government/news/new-ten-year-plan-to-make-britain-a-global-ai-superpower>. Acesso em: 27 abr. 2023

GIL, A. A. C. Como elaborar projetos de pesquisa. [s.l.] Éditeur: São Paulo: Atlas, 2010.

GITLIN, J. M. **The US Air Force successfully tested this AI-controlled jet fighter**. Disponível em: <https://arstechnica.com/cars/2023/02/the-us-air-force-successfully-tested-this-ai-controlled-jet-fighter/>. Acesso em: 26 abr. 2023.

MARKETS AND MARKETS. **Intrusion Detection and Prevention Systems Market Growth Drivers & Opportunities |** MarketsandMarkets. Disponível em: <https://www.marketsandmarkets.com/Market-Reports/intrusion-detection-prevention-system-market-199381457.html>. Acesso em: 25 abr. 2023.

ITÁLIA. **Strategic Programme on Artificial Intelligence**. Disponível em: <https://assets.innovazione.gov.it/1637777513-strategic-program-aiweb.pdf>. Acesso em: 26 abr. 2023.

INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO. **Planos estratégicos de desenvolvimento de Inteligência Artificialitsrio.org**. [s.l: s.n.]. Disponível em: <https://itsrio.org/wp-content/uploads/2020/03/RelatorioAI.pdf>. Acesso em: 26 abr. 2023.

JANIESCH, C.; ZSCHECH, P.; HEINRICH, K. Machine learning and deep learning. **Electronic Markets**, v. 31, n. 3, p. 685–695, 8 abr. 2021.

KANIMOZHI, V.; JACOB, T. Prem. **Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing**. ICT Express, v. 7, n. 3, p. 366-370, 2021.

Kaspersky Anti Targeted Attack Platform | Kaspersky. Disponível em: <https://www.kaspersky.com/enterprise-security/anti-targeted-attack-platform>. Acesso em: 26 abr. 2023.

KELLEY, A. **U.S.-Mexico Cyber Talks Begin With Focus On Critical Infrastructure**. Disponível em: <https://www.nextgov.com/cybersecurity/2022/08/us-mexico-cyber-talks-begin-focus-critical-infrastructure/376153/>. Acesso em: 25 abr. 2023.

KHRAISAT, A. et al. **Survey of intrusion detection systems: techniques, datasets and challenges**. Cybersecurity, v. 2, n. 1, p. 1–22, dez. 2019.

KIM, F. **South Korea enhances defense with robotics, AI systems.** Disponível em: <https://ipdefenseforum.com/2022/09/south-korea-enhances-defense-with-robotics-ai-systems/#:~:text=Faced%20with%20a%20shrinking%20labor%20pool%20and%20threatening,National%20Defense%20%28MND%29%2C%20known%20as%20Defense%20Innovation%204.0.>. Acesso em: 26 abr. 2023.

KONAEV, M. **06 Military applications of artificial intelligence: the Russian approach.** Disponível em: <https://www.chathamhouse.org/2021/09/advanced-military-technology-russia/06-military-applications-artificial-intelligence>. Acesso em: 27 abr. 2023.

LE FEVRE CERVINI, E. M. **And off we go, Italy launches the Strategic Programme on Artificial Intelligence 2022-2024**. 26 nov. 2021.

LEYS, N. Autonomous Weapon Systems and International Crises Strategic Studies Quarterly ♦. [s.l: s.n.]. Disponível em: <https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-1/Leys.pdf>. Acesso em: 26 abr. 2023.

MEXICO NEWS DAILY. **Mexico is vulnerable to foreign cyberattacks, says former US official.** Disponível em: <https://mexiconewsdaily.com/news/mexico-cyberattacks-china-russia/>. Acesso em: 25 abr. 2023.

OBIS, A.; MACRI, K. The 2023 **NDAA Emphasizes AI Investment for Cybersecurity, JADC2.** Disponível em: <https://governmentciomedia.com/2023-ndaa-emphasizes-ai-investment-cybersecurity-jadc2>. Acesso em: 25 abr. 2023.

OSAWA, J. **How Japan Is Modernizing Its Cybersecurity Policy** • Stimson Center. Disponível em: <https://www.stimson.org/2023/japan-cybersecurity-policy/>. Acesso em: 26 abr. 2023.

PINTO, A. et al. Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure. **Sensors**, v. 23, n. 5, p. 2415–2415, 22 fev. 2023.

PORTNOY, G. Gaby Portnoy, **Director General of Israel National Cyber Directorate at CyberWeek: We are Promoting a National Cyber-Dome**. , 6 2022. Disponível em: <https://www.gov.il/en/Departments/news/cyberweek2022>. Acesso em: 25 abr. 2023

POUSSIELGUE, G. **Macron à l'épreuve de la montée des tensions sociales.** Disponível em: <https://www.lesechos.fr/2018/03/emmanuel-macron-annonce-un-plan-de-15-milliard-deuros-pour-lintelligence-artificielle-985382>. Acesso em: 26 abr. 2023.

REBELLO, G. A. F. et al. **Sistemas de Detecção de Intrusão**. Disponível em: <https://www.gta.ufrj.br/grad/16_2/2016IDS/conceituacao.html>. Acesso em: 28 mar. 2023

RICH, E.; KNIGHT, K. **Artificial intelligence**. 2.ed. s.l.: McGraw-Hill, 1991

ROBERTS, H. et al. **The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation**. AI & society, v. 36, n. 1, p. 59–77, 2021.

SAATY, T. L. **Theory and applications of the analytic network process : decision making with benefits, opportunities, costs, and risks**. Pittsburgh, Penn.: Rws Publications, 2009.

SAEED, A. **Artificial intelligence and modern warfare: Comparative analysis of India and Pakistan**. Disponível em: <https://moderndiplomacy.eu/2023/04/07/artificial-intelligence-and-modern-warfare-comparative-analysis-of-india-and-pakistan/>. Acesso em: 27 abr. 2023.

SARANYA, T. et al. Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review. **Procedia Computer Science**, v. 171, p. 1251–1260, 2020

SAUER, F. **Artificial Intelligence in the Armed Forces On the need for regulation regarding autonomy in weapon systems.** [s.l: s.n.]. Disponível em: <https://www.baks.bund.de/sites/baks010/files/working_paper_2018_26.pdf>. Acesso em: 26 abr. 2023.

SICHMAN, J. S. **Inteligência Artificial e sociedade: avanços e riscos. Estudos Avançados**, v. 35, n. 101, p. 37–50, abr. 2021.

THORNTON, D. **CYBERCOM surveying DoD machine learning requirements to prioritize future investments.** Disponível em: <https://federalnewsnetwork.com/defense-main/2022/06/cybercom-surveying-dod-machine-learning-requirements-to-prioritize-future-investments/>. Acesso em: 26 abr. 2023.

TIDY, J. **Guerra na Ucrânia**: os três ciberataques russos que as potências ocidentais mais temem. BBC, 27 mar. 2022.

UNITED KINGDOM. Defense and security accelerator. **IFA039 - AI For Defence**. Disponível em: <https://www.gov.uk/government/publications/defence-and-security-accelerator-dasa-open-call-for-innovation/ifa039-ai-for-defence>. Acesso em: 27 abr. 2023.

UNITED STATES. **The National Artificial Intelligence Initiative (NAII)**. Disponível em: <https://www.ai.gov/>. Acesso em: 26 abr. 2023.

UNITED STATES. United States Cyber Command. **Technical Challenge Problems Guidance,** 12 mar 2019. Disponível em: https://www.cybercom.mil/Portals/56/Documents/Technical%20Outreach/Technical%20Challenge%20 Problems.pdf?ver=2019-07-02-151118-497. Acesso em: 25 abr. 2023.

U.S. DEPARTMENT OF DEFENSE. **Responsible Artificial Intelligence Strategy and Implementation Pathway**. Jun 2022. Disponível em: <https://www.ai.mil/docs/RAI_Strategy_and_Implementation_Pathway_6-21-22.pdf>. Acesso em: 25 abr. 2023

WILLIAM, D. **How AI can help improve intrusion detection systems**. Disponível em: <https://gcn.com/cybersecurity/2020/04/how-ai-can-help-improve-intrusion-detection-systems/291266/>. Acesso em: 25 abr. 2023.

ZAHRA, A. A.; NURMANDI, A. The strategy of develop artificial intelligence in Singapore, United States, and United Kingdom. **IOP conference series. Earth and environmental science**, v. 717, n. 1, p. 012012, 2021.

APPENDIX A

Top 15 largest economies according to GDP (2021)

Country	GDP (in trillions of dollars)
United States	22,67
China	16,14
Japan	5,15
Germany	4,29
United Kingdom	2,95
India	2,91
France	2,86
Italia	2,13
Canada	1,85
South Korea	1,83
Russia	1,66
Australia	1,43
Spain	1,42
Brazil	1,29
Mexico	1,21

Source: Adapted from IMF (2023)