CAPÍTULO 3

A UTILIZAÇÃO DE INTELIGÊNCIA ARTIFICIAL COMO ESTRATÉGIA DE DEFESA NACIONAL

Data de submissão: 09/02/2024 *Data de aceite: 01/04/2024*

João Pedro Santos Nanni
Graduando do Curso de Formação de Oficiais Intendentes (CFOInt) da Academia da Força Aérea (AFA), atualmente, cursando a terceira série
Academia da Força Aérea
Pirassununga - São Paulo

Gabriel Almeida de Azevedo
Graduando do CFOInt da AFA, cursando a terceira série
Academia da Força Aérea
Pirassununga - São Paulo

Daniel Torres Farias Alencar
Graduando do CFOInt da AFA, cursando a terceira série
Academia da Força Aérea
Pirassununga - São Paulo

Koffi Arnold Apolinarie Kini
Graduando do Curso de Formação de Oficiais Aviadores (CFOAv) da AFA, cursando a terceira série
Academia da Força Aérea
Pirassununga - São Paulo

Homero Henrique Nepomuceno Bortolussi
Graduando do CFOInt da AFA, cursando a segunda série
Academia da Força Aérea
Pirassununga - São Paulo

Guilherme Augusto Spiegel Gualazzi
Professor de Tecnologias da Informação, Sistemas de Informação e Cibernética da AFA
Academia da Força Aérea
Pirassununga - São Paulo

RESUMO: Considerando o desenvolvimento em velocidade cada vez maior da tecnologia de Inteligência Artificial, tornou-se evidente a sua influência nas Capacidades de Defesa Nacional. Nesse contexto, vislumbra-se a possibilidade de utilizar um sistema inteligente para suprir essas capacidades. Com o avanço da tecnologia e da inteligência artificial, estabeleceu-se uma relação entre o sistema de aprendizado, conhecido como "*machine learning*", e os diversos sistemas de defesa como Sistemas de Detecção de Intrusão, Reconhecimento e Identificação de Características. É importante destacar que os setores envolvidos nesse método constituem parte da política de defesa nacional de seus respectivos países, reforçando a relevância de uma análise minuciosa sobre sua importância no cenário mundial. Diante disso, o presente trabalho objetiva realizar uma análise abrangente do

panorama mundial dos sistemas que utilizam técnicas de inteligência artificial no âmbito da defesa nacional. Para tanto, restringiu-se o espaço amostral ao estudo das quinze maiores economias de 2022, analisando artigos científicos, relatórios de instituições especializadas e notícias de ampla divulgação.
PALAVRAS-CHAVE: Defesa Nacional, Inteligência Artificial (IA), Aprendizado de Máquina.

THE USE OF ARTIFICIAL INTELLIGENCE AS A NATIONAL DEFENSE STRATEGY

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 intelligent systems to fulfill these capabilities is envisioned. With the advancement of technology and Artificial Intelligence, a relationship has been established between the learning system, known as “machine learning”, and various defense systems such as Intrusion Detection Systems, Feature Identification and Recognition. It is important to note 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 in the global scenario. In light of this, this paper aims to conduct a comprehensive analysis of the world panorama of systems that use Artificial Intelligence techniques in the context of national defense. To this end, the sample space was restricted to the study of the fifteen largest economies of 2022, analyzing news items, reports, and scientific articles.
KEYWORDS: National Defense, Artificial Intelligence (AI), Machine Learning (ML).

INTRODUÇÃO

A utilização da Inteligência Artificial (IA) tem se tornado cada vez mais presente em diversas áreas da sociedade. Segundo relatório da Markets and Markets (2022), o mercado de IA está projetado para crescer de US$ 86,9 bilhões, em 2022, para US$ 407 bilhões, em 2027. Uma das áreas que têm explorado suas potencialidades é a Defesa Nacional, com países como Estados Unidos, China e Rússia desenvolvendo pesquisas nesse tema (BARREIROS et al, 2021). Visando aprimorar a segurança e a proteção do país, a IA tem sido utilizada como estratégia para auxiliar em diversas atividades, como a detecção de ameaças, a tomada de decisões e o planejamento de operações militares.

A IA não possui uma definição formal que seja amplamente aceita, já que para Rich e Night (1991), conceituar esse tema seria uma efemeridade por se referir a uma área da computação, e assim falhar em englobar uma nova área. Para Sichman (2021), o que se torna apropriado é a definição de seus objetivos. “O objetivo da IA é desenvolver sistemas para realizar tarefas que, no momento, são mais bem realizadas por seres humanos que por máquinas, ou não possuem solução algorítmica viável pela computação convencional.” (RICH E NIGHT, 1991, *apud* SICHMAN, 2021).

De acordo com Sichman (2021), a história da IA remonta a década de 1950, e o próprio desenvolvimento da computação. O primeiro marco nesse desenvolvimento foi dado

em 1956, com a realização da *Darthmouth College Conference*, nos Estados Unidos, que reuniu diversos especialistas para discutir a criação de softwares que pudessem simular a inteligência humana.

A IA tem se desenvolvido exponencialmente nas últimas 6 décadas, tornando-se uma tecnologia amplamente presente em áreas como Saúde, Indústria e Cidades Inteligentes, como os enfoques dos Centros de Pesquisa Aplicados promovidos pelo governo brasileiro segundo o Ministério da Ciência, Tecnologia e Inovação (BRASIL, 2021). Na Defesa Nacional, a IA tem sido utilizada para auxiliar em atividades que exigem grande precisão e rapidez, como o reconhecimento de voz, fala e facial, a detecção de movimentações suspeitas em áreas de fronteira e a análise de dados para prever possíveis ataques tanto físicos quanto cibernéticos, como mostra a Estratégia de Brasileira de Inteligência Artificial (BRASIL, 2021).

Além disso, a IA também tem sido utilizada para auxiliar em processos de tomada de decisão e governança, como mostrado na Estratégia Brasileira de Inteligência Artificial, permitindo que os militares tenham acesso a informações relevantes de forma rápida e precisa. Isso pode ser particularmente útil em situações de conflito, em que a rapidez e a precisão das informações podem fazer a diferença entre o sucesso e o fracasso de uma operação.

No entanto, a utilização da IA na Defesa Nacional também apresenta desafios e ameaças. Para Dietterich e Horvitz (2015), e como retomado por Sichman (2021) existem 5 grandes conjuntos de riscos:

1. Erros de *software*: todos os sistemas estão sujeitos aos bugs, porém esses em sistemas críticos podem estar acompanhados de grandes custos e mortes resultantes.
2. Proteção cibernética: assim como os demais sistemas computacionais e softwares, os sistemas de IA são vulneráveis a ataques cibernéticos.
3. Aprendiz de feiticeiro: assim como no conto do aprendiz de feiticeiro, a IA deve ser capaz de analisar o comando dado, não executando atividades indesejáveis devido a não razoabilidade da ordem.
4. Autonomia compartilhada: um dos desafios da implementação de sistemas de IA é a transição de responsabilidade e comando entre a máquina e seu operador.
5. Impactos socioeconômicos: a IA é capaz de influenciar todas as esferas da sociedade, causando diversos impactos que devem ser entendidos.

Uma das possíveis áreas de atuação dos sistemas que utilizam técnicas de IA, é a dos Sistemas de Detecção de Intrusão em redes de computadores, devido ao grande volume de dados e necessidade de rápida atuação. Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), de 2011 a 2020, foram reportados 6.685.512 incidentes. Essa realidade também é constante em outros países.

Além disso, o relatório da *Cybersecurity and Infrastructure Security Agency* (CISA) mostra que, em 2020, houve mais de 2000 incidentes cibernéticos que afetaram agências federais, infraestruturas críticas e outras organizações nos Estados Unidos. Essas informações corroboram a ideia de que a situação atual é um ambiente de constante conflito e ameaça para todas as instituições e nações. Portanto, essa é uma das áreas críticas que permitem a influência da IA para contribuir com a Defesa Nacional.

Nesse contexto, o objetivo do presente trabalho é analisar a utilização de Inteligência Artificial aplicada à Defesa Nacional por diversos países, colocando em evidência aqueles que possuem indicadores de utilização desses sistemas, para verificar o seu grau de importância ao nível global.

Após essa breve introdução, apresenta-se a metodologia utilizada e na sequência a fundamentação teórica que dá sustentação às análises. Na terceira seção, apresentam-se os principais resultados e uma breve discussão. As considerações finais encerram o trabalho.

METODOLOGIA

Para atingir o objetivo proposto, essa pesquisa se utiliza da pesquisa bibliográfica, em nível exploratório, como é enunciado por Gil (2010, p.44), acerca da aplicação Inteligência Artificial no âmbito das nações. Busca-se elencar indícios da utilização dessa tecnologia aplicada como ferramenta de defesa e colocá-la sob a ótica da Estratégia de Defesa Nacional. Optou-se por analisar as 15 maiores economias em 2022, conforme anexo A. Essa quantidade se justifica para incluir Brasil e México e considerar esses dois países latino-americanos em perspectiva com as demais nações de PIB mais elevado. Para além das 15 nações, foram incluídos Estados identificados como expoentes na área. Fundamentalmente, buscou-se como fontes bibliográficas, conforme as categorias enunciadas por Gil (2010, p.44):

a. O arcabouço científico de publicações periódicas usando como palavras-chave: Defesa Nacional, Inteligência Artificial (IA). Os artigos foram retirados, fundamentalmente, de plataformas como SciElo, Science Direct e Springer.

b. Os livros de leitura corrente, os quais caracterizados como obra de divulgação, e os livros de referência.

c. Impressos diversos como:

    a. Relatórios de incidentes, retirados de plataformas como do CGI.br, CISA.

    b. Registros jornalísticos, pois são entendidos como uma fonte de informação com menor intervalo de tempo entre o acontecimento e sua publicação, quando comparados aos artigos científicos. Esses foram retirados de diversas plataformas, como citado na bibliografia, do período compreendido entre 2013 e 2023.

FUNDAMENTAÇÃO TEÓRICA

A Estratégia Nacional de Defesa é um conjunto de ações coordenadas pelo Estado para garantir a proteção do território e da população contra ameaças externas. Ela é composta por um conjunto de políticas, medidas, planos e ações que visam garantir a segurança nacional em diversas áreas, como a defesa militar, a segurança das fronteiras, a segurança cibernética e a defesa contra ameaças químicas, biológicas, radiológicas e nucleares. E por meio desses, garantir os objetivos descritos no Plano Nacional de Defesa (BRASIL, 2022).

Os sistemas de Inteligência Artificial são utilizados em diversas nações, dentre os usos que são correlatos às competências esperadas dentro da Defesa Nacional. Para a Estratégia Nacional de Defesa (BRASIL, 2022), as capacidades são as de: Proteção, Pronta-resposta, Dissuasão, Coordenação e Controle, Gestão de Informação, Logística para Defesa Nacional, Mobilidade Estratégica, Mobilização e Desenvolvimento Tecnológico de Defesa.

A Inteligência Artificial para Allen e Chan (2017), consegue desenvolver habilidades abrangentes de resolução de problemas em seus próprios algoritmos, o que a faz crescer de forma exponencial. (CÔRREA, 2021). Para Janiesch *et al*. (2021) as técnicas de *Machine Learning* podem ser sintetizadas como os sistemas que buscam automaticamente aprender com relações e padrões significantes provenientes de exemplos e observações. E com os avanços nessa tecnologia, já é possível identificar, em meio à sociedade, a ascensão dos sistemas inteligentes com cognição análoga à humana.

De acordo com Janiesch *et al*. (2021), os algoritmos de *Machine Learning* se destacam nas aplicações de regressão, agrupamento e classificação, sendo dependentes dos conjuntos de dados de problemas específicos para serem capazes de compreender as correlações e nuances da atividade a ser executada. Dessa forma, eles se destacam nas atividades como *next-best offer analysis* (NBO), identificação de padrões ou exceções, como detecção de documentos fraudulentos, reconhecimento de emoções, comportamentos, fala e imagem, bem como *natural language processing* (NLP).

Segundo Chen *et al*. (2023), Técnicas de *ML* podem ser utilizadas na análise dos dados resultantes do imageamento, como na classificação *hyperspectral images* (HSIs)., sendo a partir disso, capaz de identificar precisamente o terreno, com suas propriedades, como relevo, vegetação, recursos e instalações. Esse tipo de análise fornece dados vitais para a Defesa Nacional, principalmente quando aplicado no teatro de operações.

Como identificado na Estratégia Brasileira de Inteligência Artificial (BRASIL, 2021), os sistemas de IA fornecem grande auxílio à decisão ao gestor. Essa influência impacta, então, diretamente partes componentes das Forças Armadas, como as atividades de Comando e Controle.

Além disso, para Leys (2018) a IA pode ser utilizada em *Autonomous Weapon Systems (AWS)*, o quais são capazes de operar ou não em conjunto com o humano, e quando independente, pode aprimorar os tempos de reação e o período de disponibilidade. Ademais essa situação, em condições de perda de comunicação, os sistemas de *AWS*, diferentemente dos remotamente controlados, são capazes de manter suas capacidades operacionais frente aos diferentes cenários que possam ser encontrados, sendo esse um objetivo integrante do Plano de Articulação de Equipamentos de Defesa na Estratégia Nacional de Defesa (BRASIL, 2021).

Outra aplicação da IA na Defesa Nacional é a análise de dados para prever situações de conflito. Através da análise de inteligência, a IA pode identificar tendências e padrões que possam indicar uma situação de conflito iminente, permitindo que a Defesa Nacional tome medidas preventivas ou de resposta antecipada. Além disso, a IA pode ser usada para monitorar a atividade de grupos terroristas e prever ataques desses.

As técnicas de IA podem ser utilizadas também nos Sistemas de Detecção de Invasão, tanto relativos à invasão de áreas físicas, quanto de ambientes cibernéticos. Para Saranya *et al.* (2020, p. 2), com o grande volume e velocidade da circulação de dados, os métodos tradicionais de detecção de dados não são capazes de detectar intrusos do modo mais rápido. Tendo isso em vista, a fim de possibilitar a eficiente identificação dos ataques, a partir da análise do tráfego de rede, o Sistema de Detecção de Invasão pode se utilizar de algoritmos de *ML*, os quais podem ser conceituados como a programação de computadores para otimizar critérios de desempenho usando dados de exemplo ou experiências anteriores, de acordo com Alpaydin (2020). Tendo um modelo definido com alguns parâmetros, o aprendizado é a execução de softwares para otimizar essas variáveis do modelo utilizando de dados de exemplo ou aprendizados anteriores.

A utilização de Sistemas de ML influência em diversas áreas, sendo citado na Estratégia Brasileira de Inteligência Artificial (BRASIL, 2021) o conhecimento de que a tecnologia de Inteligência Artificial se destaca no uso em Sistemas de Detecção de Intrusão. Como destacado no gráfico abaixo (FIGURA 1), os métodos de IDS, baseados em ML, possuem alta acurácia, como mostrado em Saranya et al. (2020), sendo um diferencial entre os demais métodos.

Diante dos fatos apresentados, vale ressaltar que, em 2018, o principal uso de inteligência artificial já era na área de detecção e bloqueio de intrusos, vital para a Defesa Nacional, como mostra a figura 1.

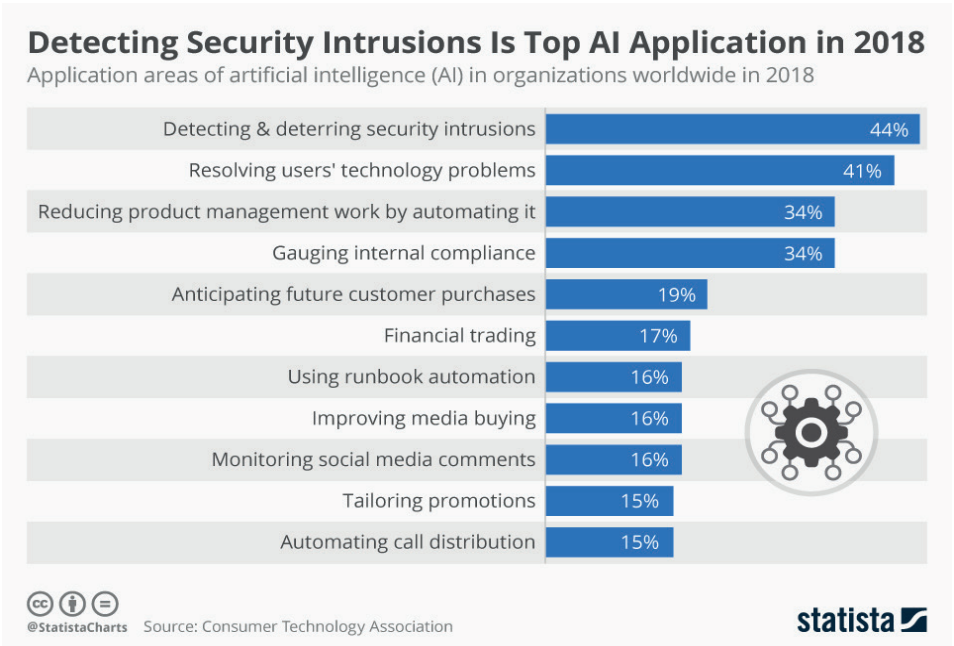

FIGURA 1 Áreas da Aplicação de Inteligência Artificial em 2018

Fonte: FELDMAN (2018). Disponível em: Detecting Security Intrusion is top AI Application in 2018

RESULTADOS E DISCUSSÃO

Os dados dos países a seguir apresentam assimetria acerca da quantidade de conteúdo apresentada. Isso ocorre devido ao maior volume de dados e referências encontrado de alguns países, por atuarem de forma mais presente no cenário internacional, o que é de se esperar em função do seu avanço tecnológico e esforços na área de defesa. De acordo com *Carnegie Endowment for International Peace* (2019), os países que têm maior capacidade para prover essa tecnologia são Estados Unidos e China. O relatório também mostra a presença de outras nações no cenário. Ao final é apresentado o item 5.17 que concatena os resultados dispostos em cada país.

Estados unidos

Segundo o relatório da Markets and Markets (2020), os Estados Unidos têm o maior mercado para IDS e agências do governo, como o Departamento de Defesa (DoD) e a Agência Nacional de Segurança (NSA), estão usando *ML* para melhorar suas capacidades cibernéticas.

Segundo Obis e Macri (2022), o *National Defense Authorization Act* (*NDAA*) de 2023 enfatizou o desenvolvimento de Inteligência Artificial, com enfoque de continuar a aceleração da tecnologia, como já vem ocorrendo, e sendo uma prioridade esse desenvolvimento na

chamada *Joint All-Domain Command-and-Control* (JADC2), sendo o simpósio de julho de 2022 motivado pela pergunta de como manter os elementos do JADC2 em estado da arte. O NDAA 2023 também estabeleceu um plano de implementação de 5 anos para os sistemas de Inteligência Artificial dentro das missões de Guerra Cibernética. “Em sua plenitude, isso [Inteligência Artificial] irá impactar o gerenciamento de vulnerabilidades, busca de ameaças e impulsionar a segurança de rede.”(apud. OBIS; MACRI, 2022, tradução nossa).

O *United States Cyber Command* (2019) também reconhece, no *Technical Challenge Problems Guidance*, como seu 15º problema desafiador que é interesse do *USCC* o uso de *ML* para caracterização de detecção de malwares desconhecidos em redes de computadores. Sendo o 17º problema desafiador relacionado a implementação desses sistemas de Inteligência Artificial. O *Responsible Artificial Intelligence Strategy and Implementation Pathway* prevê que a utilização de *ML* na detecção de ataques é um dos passos necessários no plano de implementação das ferramentas de IA.

De acordo com Thornton (2022, tradução nossa), “Dave Frederick, diretor-executivo do *CYBERCOM*, disse que o *DoD* já integrou as aplicações e produtos comercialmente disponíveis básicos em sua missão de defesa cibernética.”. Inclusive utilizando para reduzir a carga de trabalho de analistas cibernéticos, na identificação de malwares. Esse recorte elucidado por Thornton mostra o objetivo dos Estados Unidos na utilização de um *IDS* baseado em *ML*.

Segundo Gitlin (2023), a Força Aérea dos Estados Unidos (USAF) já adquiriu a capacidade de utilizar aeronaves como um F-16 modificado, X-62, de modo autônomo, tendo capacidades básicas das aeronaves como pouso e decolagem. Já o National Artificial Intelligence Initiative prevê o investimento e desenvolvimento da Inteligência a fim de manter os Estados Unidos na liderança do desenvolvimento dessa tecnologia.

China

A China investiu fortemente na última década no desenvolvimento de ML e de inteligência artificial, a proteção cibernética não é uma exceção a isso. Seu desdobramento se dá visando principalmente a Competitividade Internacional, visto como um projeto estratégico. De acordo com *Carnegie Endowment for International Peace* (2019), a China é o maior veiculador das Tecnologias de IA, além de utilizar tecnologias tanto provenientes de sua própria nação quanto as dos Estados Unidos, possuindo tanto tecnologias de reconhecimento facial, quanto de Cidades e Policiamento Inteligentes.

Segundo Roberts *et al* (2021), em 2017 foi publicado o Plano de Desenvolvimento de Inteligência Artificial de Nova Geração, o qual é um documento que unifica e descreve os objetivos chineses quanto à IA, para isso estabelece diversos objetivos sobre o assunto, destaca se a meta do país se tornar o líder mundial em inovação de Inteligência Artificial até 2030.

A documentação destaca três áreas de importância: a primeira é a competição internacional, como parte de proporcionar saltos em sua capacidade militar, principalmente para fazer frente ao poderio militar americano usando táticas de guerra assimétrica, e dentro desse termo a ciberguerra. A segunda área é o desenvolvimento econômico, estabelecendo a IA como a força motora por trás de um novo ciclo de transformação industrial, embora exista a possibilidade da mesma perturbar as relações no mercado de trabalho. A última área é a governança social, a China vem enfrentando problemas sociais emergentes devido ao envelhecimento da população, uso de recursos naturais, etc, e para superá-los a legislação prevê o uso de IA para gerenciamento de serviços públicos buscando precisão e a melhora da qualidade de vida.

Japão

O Governo japonês, através da Estratégia de Segurança Nacional e sua posterior revisão com as observações feitas na Guerra da Ucrânia, define suas prioridades no médio e longo prazo. As duas principais modificações trazidas pela revisão, no tocante à cibersegurança, são o desenvolvimento de uma postura para guerra de informações e a introdução de uma ciberdefesa ativa. A segunda modificação dá o poder para o governo japonês de defender infraestruturas essenciais, retaliar no ciberespaço e neutralizar atacantes, para isso.

Existem ainda diversas iniciativas motivadas pelo Estado, que focam em promover o desenvolvimento de inteligência artificial na proteção cibernética, incluindo o plano “Cyber Security Vision”, que tem como um dos focos essa tecnologia

Segundo Osawa (2023), o Japão, com a nova Estratégia de Segurança Nacional, planeja aprimorar a monitoração do espaço informacional e fortalecer a análise de inteligência. Além de planejar a implantação de um sistema de coleta e análise de informações utilizando IA para auxiliar na consciência do campo de batalha.

Alemanha

Segundo o panorama (BRASIL, 2022b), a Alemanha pretende se consolidar como referência no setor de IA, ainda ressaltando na estratégia, 12 campos de ação e 14 metas. Nesses pontos elencados, ressalta a atuação dos centros de competência do Escritório Federal para Segurança da Tecnologia da Informação (BSI), em alemão *Bundesamt für Sicherheit in der Informationstechnik*, para reunir a expertise e fornecer a consultoria acerca da segurança da informação tanto para IA, quanto por meio da IA, além da defesa contra ataques sejam assistidos por IA.

As forças armadas alemãs são uma das únicas do mundo a possuir uma unidade organizacional dedicada à defesa cibernética, em inglês chamado de *Cyber and Information Domain Service*.

O governo alemão implementou diversas medidas para aumentar suas capacidades de proteção cibernética, incluindo o uso de ML-based IDS. Em 2020, o Escritório Federal para Segurança da Tecnologia da Informação (BSI), em alemão *Bundesamt für Sicherheit in der Informationstechnik*, lançou um projeto para testar a efetividade dessa tecnologia. Essa iniciativa envolveu analisar cenário de tráfego de rede e identificação de ameaças em tempo real.

Ainda há, no país, institutos de pesquisa e empresas que estão desenvolvendo e fornecendo sistemas de proteção cibernética com essa tecnologia, como o Instituto Fraunhofer para Segurança da Tecnologia da Informação (SIT).

Segundo Sauer (2018), as forças armadas alemãs já estão desenvolvendo sistemas baseados em tecnologia de Inteligência Artificial com foco em áreas como a obtenção de *AWS.*

Reino unido

O *Department for Digital, Culture, Media & Sport* (2022) anunciou que o Reino Unido tem implementado diversas medidas para aumentar suas capacidades de proteção cibernética, incluindo o uso de ML nos sistemas de IDS. Em 2020, o Centro Nacional de Segurança Cibernética do Reino Unido (NCSC) publicou um relatório sobre o uso de IA na proteção cibernética. Esse relatório destaca os potenciais benefícios do uso desses sistemas na detecção e resposta a ameaças cibernéticas em tempo real.

De acordo com Zahra (2021), os setores de educação do Reino Unido produzem muitas publicações sobre IA. No período de 2010 a 2020, estes setores contribuíram com 1.400 iniciativas de pesquisa para desenvolver o sistema de Inteligência Artificial.

De acordo com o Reino Unido (2023), o país também financiou grupos de pesquisa e desenvolvimento de projetos focados em IDS baseados em IA. Um dos financiadores, por exemplo, o UK Defense and Security Accelerator (DASA) proveu financiamento para diversos projetos nessa área com IDS e IPS, incluindo os de ML.

Índia

Segundo SAAED (2023), foi estabelecido em 2022, o *Defence Artificial Intelligence Council (DAIC),* subordinado ao ministério da defesa indiano, tem por objetivo oferecer guiamento e incentivo para inovações que contém tecnologia avançada, visando criar 25 produtos de AI para a indústria de defesa até 2024. Outra criação recente é o *Military AI Project Agency (DAIPA)*, com mais de 13 milhões de dólares de orçamento anual, possui enfoque em projetos de auxílio ao processo decisório, segurança de fronteiras e sistemas autônomos, como drones e veículos terrestres.

França

De acordo com Poussielgue (2018), como reflexo dessa promoção, em 2018 o presidente Emmanuel Macron anunciou que o país investirá 1,5 bilhões de euros em pesquisa sobre AI nos próximos 5 anos. Inaugurado em 2022, o campus de cibersegurança em Paris é um edifício que reúne mais de 1700 profissionais da área, com origens militares e na indústria , ele tem o objetivo de ser um *hub* de pesquisa e treinamento da área visando unificar os esforços para uma melhor resposta aos ataques cibernéticos.

Itália

Segundo Cervini (2021), a IA da Itália é inspirada no Plano Coordenado da União Européia sobre IA. O governo italiano faz parte do esforço conjunto para melhorar a harmonia de regras proposta pelo regulamento europeu de IA.

Além disso, o governo italiano, por meio do Ministério da Inovação Tecnológica e Transição Digital (MITD), formulou o Programa Estratégico de Inteligência Artificial, que tem como finalidade desenvolver um ecossistema de inteligência Artificial, aumentar o financiamento para pesquisas na área e incentivar a aplicação da IA tanto na administração pública, quanto no setor privado.

O Programa Estratégico de Inteligência Artificial (ITÁLIA, 2022) define a defesa nacional como setor prioritário para o desenvolvimento de IA e afirma que o país comprometeu-se a investir na segurança cibernética nacional, na qual a IA contribuirá para a nova geração de softwares de detecção de ameaças.

Segundo Bozzetti *et al.* (2021), o Observatório de ataques digitais (OAD) é a única pesquisa online independente na Itália sobre os ataques intencionais nos sistemas de tecnologia da informação de companhias e órgãos públicos e, nesse país, os ataques cibernéticos constituem um risco crescente e sério.

Visto isso, Bozzetti *et al.* (2021) afirma que, na pesquisa OAD realizada em 2020, essa demonstrou uma melhoria das medidas de segurança digital no país, no entanto, as técnicas de prevenção, proteção e gerenciamento de inteligência artificial mais modernas ainda estão no estágio inicial de desenvolvimento entre os entrevistados.

Canadá

Segundo Khraisat (2019), em 2018, foi gerado o CSE-CIC-IDS 2018, o conjunto mais recente e realista de dados cibernéticos do Canadian Establishment for Cybersecurity (CIC) até então. Os conjuntos de dados do CIC têm sido utilizados em todo o mundo para detecção de intrusão e antecipação de malware.

O principal objetivo desses dados é construir de modo ordenado um jeito de lidar com a diferente produção e o longo alcance dos conjuntos de dados de benchmark para a detecção de intrusos na formação dos perfis de cliente, os quais contêm representações teóricas de ocasiões e práticas vistas no sistema.

Coreia do sul

De acordo com Kim (2022), o governo sul-coreano está se voltando para sistemas baseados em IA para aprimorar as capacidades das forças armadas, como estratégia de defesa. Devido a fatores como a redução da taxa de natalidade, as autoridades estão investindo na inovação de defesa 4.0.

Rússia

Segundo Konaev (2021), a Rússia desenvolve IA aplicada no ambiente militar em diversas abordagens, compondo dentre elas: guerra eletrônica, o país vem se desenvolvendo desde 2009, sendo agregadas as técnicas de IA para aumentar sua efetividade na classificação de sinais e tradução de informações; sistemas não-tripulados, a Rússia desenvolve veículos não-tripulados para todos os 4 ambientes físicos de combate moderno, como exemplo do Veículo Aéreo Não-Tripulado S-70; superioridade informacional e guerra cibernética.

Austrália

Segundo Devitt et al. (2022) a Austrália está buscando atingir a capacidade de operar AWS, inclusive com a operação autônoma de aeronaves. A proposta de uso dessas técnicas de AI, também perpassa a competência de Comando e Controle.

Espanha

Na Espanha, foi criado em 2006 o *Centro Criptológico Nacional (CCN),* incumbido de proteger sistemas, públicos ou privados, de importância estratégica de ciberataques. O mesmo também é responsável por coordenar o uso de AI para sua missão, segundo o Próprio CCN-CERT (2022).

Brasil

No início de 2021, foi criada a Estratégia Brasileira de Inteligência Artificial (EBIA). Neste documento consta que em uma Estratégia Nacional de IA deve visar desenvolver esta e utilizá-la para que o cenário científico possa evoluir e procurar resolver determinadas problemáticas palpáveis do país. Para isso, seria feita uma análise e definido quais seriam as maiores prioridades segundo a sua probabilidade de gerar vantagens para a nação. De acordo com *Carnegie Endowment for International Peace* (2019), os Estados Unidos utilizam tecnologias tanto provenientes dos Estados Unidos quanto as da China, possuindo tanto tecnologias de reconhecimento facial, quanto de Cidades e Policiamento Inteligentes.

México

Segundo Dillon (2022), Christopher Krebs, ex-diretor do United States Cybersecurity and Infrastructure Security Agency, o México precisa se proteger melhor de ataques cibernéticos que poderiam ser realizados por China ou Rússia.

Sua fala é pertinente tendo em vista que, o Ministério de Defesa Nacional do México (Sedena) e o Ministério de Infraestrutura, Comunicações e Transporte (SICT) foram vítimas de um ataque cibernético realizado por um grupo de hackers ativistas chamado The Guacamaya. O grupo se infiltrou nos servidores do Sedena e roubou milhões de e-mails e documentos enquanto hackers não-identificados violaram a segurança de 110 computadores SICT e instalaram ransomware, conforme o México News Daily.

OUTRAS NAÇÕES EXPOENTES

Estônia

De acordo com European Commission (2020), o Governo é o mais expoente na Europa no quesito de integração com a internet, com 99% dos serviços disponíveis online. Além disso, entre 2019 e 2021 investiu €10 milhões a fim de implementar sua estratégia de IA. Outra capacidade, motorizada por técnicas de IA, é a análise de dados de imageamento de satélites, a qual a nação já faz uso como no Ministério da Agricultura.

SÍNTESE DO LEVANTAMENTO

A partir da revisão sistemática da literatura feita, foi possível identificar que dos 16 países levantados, 16 apresentam fortes indicativos de considerarem essa tecnologia como um dos focos nacionais de desenvolvimento ou estarem utilizando-a.

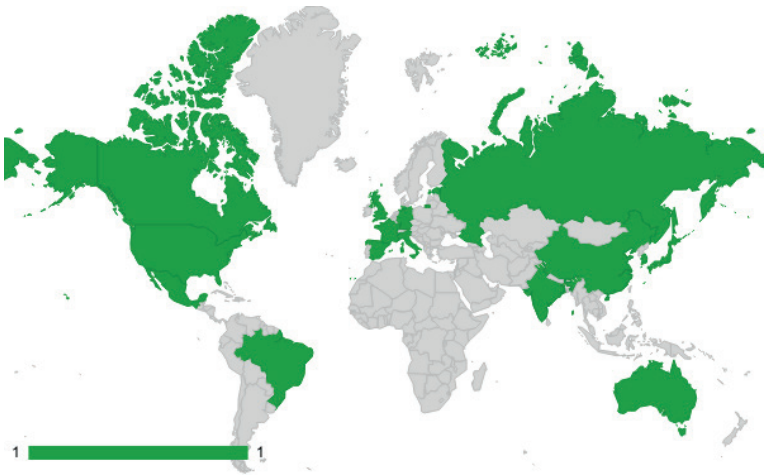

FIGURA 2 Países com Indícios da Aplicação de Inteligência Artificial em 2018

Fonte: Os autores

Os dados podem ser verificados na Figura 2, em que os países em verde são os que foram encontrados indícios de uso, e os de vermelho, os quais os indícios foram baixos. Os demais países que se encontram externos à pesquisa são apresentados na cor cinza.

Vale ressaltar que não é possível inferir se há o uso ou desenvolvimento das tecnologias dado a sensibilidade da informação acerca da capacidade defensiva.

Segundo a Estratégia Brasileira de Inteligência Artificial (BRASIL, 2021), a "IA tem também se revelado útil na prevenção e detecção de invasão de redes de computadores e de dispositivos informáticos", fato comprovado pelos relatos citados a seguir. Como exemplo elucidado pelo documento estratégico, os seguintes casos foram destacados, segundo o Darkreading (2022), em que a inteligência artificial conseguiu impedir ataques cibernéticos:

> - No início de 2022, uma empresa de capital privado que procurava reforçar seus esforços de segurança de e-mail testou uma solução de segurança de e-mail de IA e detectou um ataque de falsificação. Os invasores adaptaram seu e-mail para imitar as comunicações internas de RH da empresa. Uma investigação mais aprofundada mostrou que o e-mail faz parte de uma tendência mais ampla de campanhas de phishing direcionadas que usam marcas falsas da Microsoft para enganar os funcionários.
>
> - Em março de 2022, uma empresa sul-africana de serviços financeiros descobriu um ataque de ransomware em andamento tentando criptografar seus dados. O primeiro sinal de comprometimento foi um servidor de e-mail da empresa fazendo conexões HTTP incomuns e se comunicando com um servidor malicioso. Sua compreensão do negócio e do comportamento normal desse servidor de e-mail em particular permitiu que a IA identificasse a atividade ameaçadora.

CONCLUSÃO

Vale ressaltar que não foi o objetivo do trabalho tratar do estágio de desenvolvimento que se encontra o programa de cada país, sendo esses indícios fundamentados na utilização dos métodos de IA aplicados nas diversas áreas da defesa.

Com isso, conclui-se que, ao fazer a análise dos países neste trabalho, é verificada a importância da utilização da IA na área de Defesa Nacional, tendo em vista que cerca de 100% das nações analisadas já estão, pelo menos, dando indício de investimentos neste cenário. Utilizando os próprios relatos de bloqueio de conexões hostis pela AI mencionados anteriormente, a aplicação do ML, além de ser uma prática já com fortes indicativos de ser difundida entre as nações, é também um método que foi capaz de impedir diversos ataques de malwares.

Portanto, como a maioria das maiores nações, do ponto de vista econômico, consideram a IA uma tecnologia relevante para a Defesa Nacional e estão buscando cada vez mais fazer investimentos nessa área, pode-se aferir a importância do objeto estudado neste trabalho.

REFERÊNCIAS

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/PanoramaInternacionalPolticasNacionaiseInstitutosdeInteligenciaArtificialV2.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%20Problems.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.

APÊNDICE A

As 15 maiores economias de acordo com o PIB (2022)

País	PIB (em trilhões de dólares)
Estados Unidos	22,67
China	16,14
Japão	5,15
Alemanha	4,29
Reino Unido	2,95
India	2,91
França	2,86
Itália	2,13
Canadá	1,85
Coreia do Sul	1,83
Rússia	1,66
Austrália	1,43
Espanha	1,42
Brasil	1,29
México	1,21

Fonte: Adaptado de FMI (2023)