ESCOLA SUPERIOR DE GUERRA

LUÍS CLÁUDIO DA SILVA FARIA

O IMPACTO DA IA PARA A DEFESA CIBERNÉTICA: proposta para criação do Comando Conjunto de Inteligência Artificial

Trabalho Acadêmico – Ensaio Acadêmico apresentado ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do certificado do Curso Superior de Segurança e Defesa Cibernética.

Orientador: Ten Cel Ricardo Férre Lacerda Ferreira

Rio de Janeiro
2024

C2024ESG

Documento assinado digitalmente
gov.br
LUIS CLAUDIO DA SILVA FARIA
Data: 22/10/2024 14:33:12-0300
Verifique em https://validar.iti.gov.br

_____

LUÍS CLÁUDIO DA SILVA FARIA

RESUMO

Nas últimas duas décadas, observou-se uma rápida evolução dos meios tecnológicos e a digitalização do mundo em que vivemos, impulsionada pela internet e pelo avanço da inteligência artificial. Essa migração das atividades humanas para o meio digital tem ocorrido de forma acelerada e a inteligência artificial vem sendo empregada em todos os campos de atuação humana, inclusive no campo militar. A inteligência artificial está transformando a forma de combater e os países que dominarem essa tecnologia estarão à frente na defesa cibernética e em consequência consolidarão sua posição no poder global. O Brasil, para ocupar um espaço entre as superpotências mundiais, precisa dominar essa tecnologia, garantindo a capacidade de se defender de ataques externos. Para viabilizar esse esforço soberano é necessário unir forças, de modo que esse objetivo seja alcançado. As três Forças Armadas contam com um capital humano altamente capacitado para o desenvolvimento de novas tecnologias, porém os recursos orçamentários são limitados. Portanto, a criação de um Comando Conjunto de Inteligência Artificial pode ser o canal viabilizador dessa nova estratégia tecnológica no Brasil.

Palavras-chave: inteligência artificial; defesa cibernética; Comando Conjunto.

ABSTRACT

In the last two decades, there has been a rapid evolution of technological means and the digitalization of the world in which we live, driven by the internet and the advancement of artificial intelligence. This migration of human activities to the digital realm has been occurring at an accelerated pace, and artificial intelligence has been employed in all fields of human activity, including the military sector. Artificial intelligence is transforming the way combat is conducted, and countries that master this technology will be at the forefront of cybersecurity and will consequently consolidate their position in global power. For Brazil to occupy a space among the world superpowers, it needs to dominate this technology, ensuring its ability to defend against external attacks. To facilitate this sovereign effort, it is necessary to unite forces so that this goal can be achieved. The three Armed Forces have a highly skilled human capital for the development of new technologies; however, budgetary resources are limited. Therefore, the creation of a Joint Command of Artificial Intelligence could be the enabling channel for this new technological strategy in Brazil.

Keywords*: artificial intelligence; cyber defense; Joint Command.*

1 INTRODUÇÃO

Os avanços proporcionados pela era digital nos últimos anos são impressionantes, mudando a maneira como os seres humanos interagem com o mundo. O ambiente virtual transformou a interface entre o ser humano e a realidade. O lançamento da inteligência artificial chamada ChatGPT, desenvolvida pela OpenAI, em novembro de 2022, provocou uma explosão no uso dessa tecnologia, em apenas dois meses o número de usuários passava de 100 milhões de pessoas (Andrade, 2023).

A capacidade da computação e do processamento digital, combinada com o vasto volume de informações disponíveis, possibilita soluções eficazes de forma rápida. Isso exige que a sociedade se adapte, já que a inteligência artificial pode ser aplicada em atividades que os seres humanos não conseguem realizar, como coordenar um enxame de drones ou gerenciar a localização de várias pessoas simultaneamente, comunicando-se com diversos dispositivos de maneira rápida e precisa (Andrade, 2023).

A inteligência artificial generativa é um tipo de tecnologia que aprende e se adapta a diferentes situações. Nos conflitos armados recentes, como o entre Ucrânia e Rússia, o uso de inteligência artificial se estabeleceu como uma importante ferramenta na guerra moderna (Goncharuk, 2024).

Essa nova ferramenta está sendo usada, não apenas para operações cibernéticas, mas também na interação com equipamentos cinéticos, por exemplo, na seleção de alvos para bombardeios aéreos e executar ataques por meio de drones (Zafra; Hunder; Rao; Kiyada, 2024).

O Brasil deve participar ativamente dessa revolução tecnológica. Sendo o 5º maior país do mundo em extensão territorial e com uma população diversificada com 212,6 milhões de habitantes, o Brasil possui um enorme potencial econômico, cultural e tecnológico. A diversidade de seus recursos naturais, aliada à rica variedade cultural, proporciona uma base sólida para inovações em vários setores, incluindo tecnologia e defesa (Belandi; Campos, 2024).

Este trabalho busca analisar o impacto da inteligência artificial na defesa cibernética. O objetivo é propor uma linha de ação que viabilize o domínio dessa tecnologia para a segurança nacional, viabilizando ao país não apenas integrar essas inovações em suas práticas de defesa, mas também se tornar um protagonista no cenário global.

2 DESENVOLVIMENTO

A ideia de criar uma inteligência não-biológica é um sonho muito antigo da humanidade, bem antes de o campo da inteligência artificial ser oficialmente estabelecido em 1956. Na verdade, essa busca pode ser rastreada por séculos, ou até milênios, dependendo da definição. Durante grande parte desse tempo, o objetivo de "criar" inteligência poderia ser mais bem entendido como "projetar" inteligência (Spector, 2006).

2.1 EVOLUÇÃO DA IA

Uma das definições mais clássicas de Inteligência Artificial (IA) é o Teste de Turing, proposto pelo matemático e cientista Alan Turing. Nele, propõe que uma máquina poderia ser considerada inteligente se fosse capaz de conversar com um humano de forma indistinguível de outro humano. Em outras palavras, um humano não saberia dizer se está conversando com uma máquina ou com outro humano, então a máquina poderia ser considerada inteligente (Turing, 1950).

Já o termo "inteligência artificial" surgiu em 1956, durante a primeira conferência de IA no Dartmouth College, nos Estados Unidos, criado pelo cientista de computação John McCarthy (McCarthy; Minsky; Rochester; Shannon, 1956)

Após um período de intensas pesquisas, a IA passou por um período conhecido por "inverno da IA" da década de 1970 até o computador de xadrez Deep Blue na década de 1990 (OCDE, 2019).

A partida de xadrez ocorrida em 1997, na qual o supercomputador Deep Blue venceu o multicampeão Garry Kasparov, é um marco no desenvolvimento da Inteligência Artificial. Desde então, a IA continuou a avançar de forma acelerada, culminando, em 2011, com a criação de tecnologias que expandiriam ainda mais suas capacidades. O principal impulsionador desse avanço foi o 'aprendizado de máquina', conforme destacado pela OCDE (2019):

> “Desde 2011, avanços em "aprendizado de máquina" (ML), um subconjunto e IA que usa uma abordagem estatística, têm melhorado a capacidade das máquinas de fazer previsões a partir de dados históricos. A maturidade de uma técnica de modelagem de ML chamada "redes neurais", juntamente com grandes conjuntos de dados e poder computacional, está por trás da expansão no desenvolvimento de IA.”

Esses avanços abriram caminho para a criação de modelos de IA capazes de realizar tarefas cada vez mais complexas, transformando setores como e-commerce,

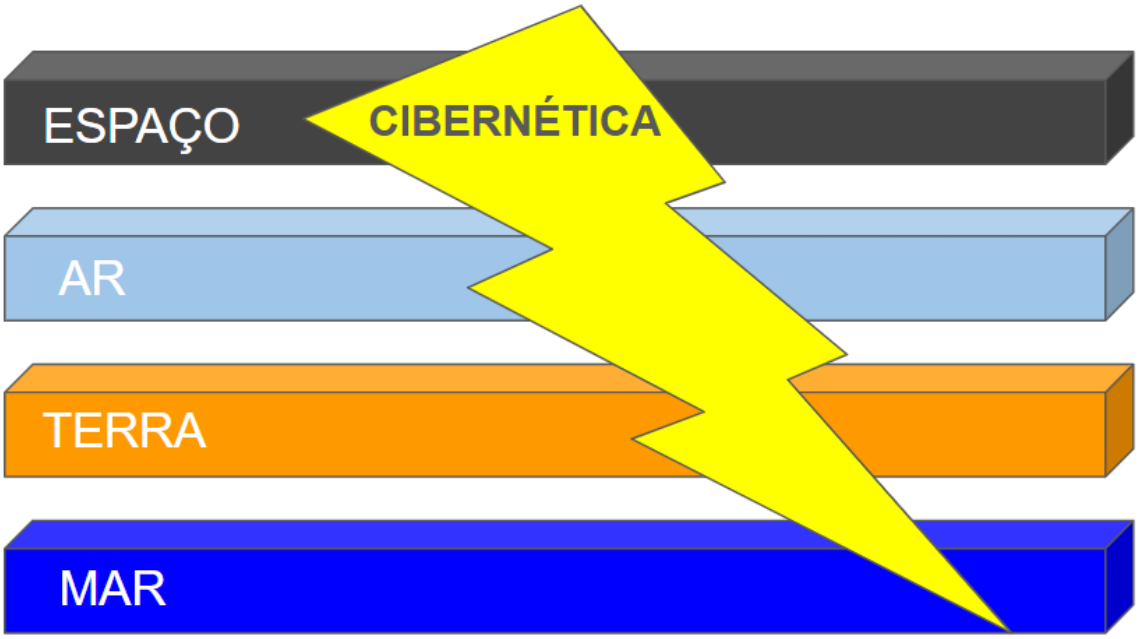
saúde, indústria, comunicação e defesa, pavimentando, assim, o caminho para o surgimento, em novembro de 2022, de ferramentas como o ChatGPT, que marcou uma nova era na interação entre humanos e máquinas (Figueiredo, 2023).

Atualmente a Inteligência Artificial (IA) atua como uma ferramenta para a cibersegurança. A tecnologia de IA possibilita a análise de grandes volumes de dados em tempo real, identificando padrões de comportamento suspeitos que seriam difíceis de serem detectados manualmente. Isso resulta em uma detecção precoce de ameaças e respostas imediatas a incidentes cibernéticos (Débora, 2024).

2.2 CIBERSEGURANÇA E CIBERATAQUES EM CONFLITOS RECENTES

O ciberespaço é um ambiente extremamente complexo, cuja principal característica é a sua capacidade de transversalidade, pois pode permear todas as dimensões. O ciberespaço não respeita as fronteiras físicas territoriais como conhecemos, por isso esse ambiente é considerado o 5º domínio da guerra (Oliveira, 2022).

Figura 1: Transversalidade da cibernética



Fonte: O autor, 2024.

Nos conflitos mais recentes podemos verificar a alta utilização de cibersegurança e os ciberataques, visando causar danos ao inimigo.

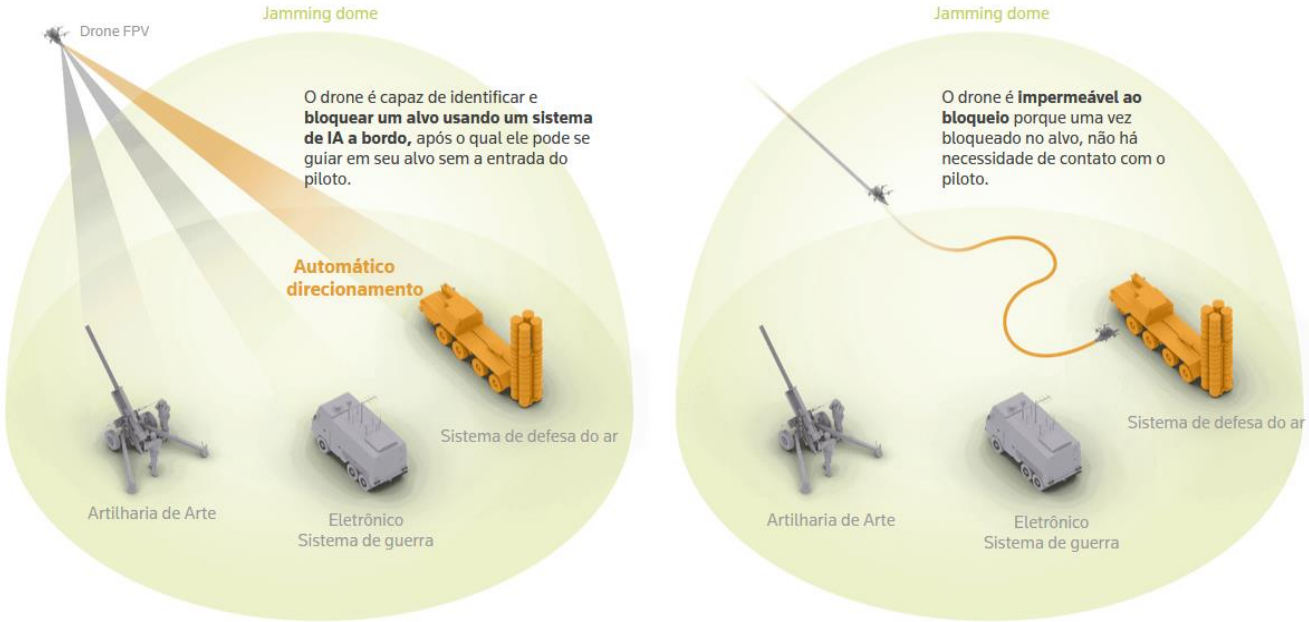
2.2.1 utilização da IA na cibernética no conflito Ucrânia x Rússia

A guerra entre Rússia e Ucrânia é um conflito que se iniciou no dia 24 de fevereiro de 2022 devido à invasão do território ucraniano pelas forças militares russas (Rosenberg, 2024).

A superioridade bélica da Rússia perante a Ucrânia, gerou expectativa de um combate rápido e com desfecho favorável ao país de Putin. Ocorre que o conflito já supera dois anos de duração e a resiliência ucraniana surpreende. Existem vários fatores que influenciam esta situação, como por exemplo o apoio dos países ocidentais (Zafra; Hunder; Rao; Kiyada, 2024).

Outro aspecto que tem sido fundamental para a resistência ucraniana é o uso estratégico de pequenos drones, equipamentos de baixo custo que podem ser adquiridos por cerca de US$ 500. Esses drones, muitas vezes adaptados de modelos comerciais, são utilizados para reconhecimento, mapeamento de terreno e até para ataques direcionados. Alguns são modificados para carregar pequenas cargas explosivas, transformando-os em armas letais de baixo custo que podem desativar recursos inimigos de valor muito mais elevado (Zafra; Hunder; Rao; Kiyada, 2024).

Figura 2: Drones guiados por IA



Fonte: Zafra; Hunder; Rao; Kiyada, 2024.

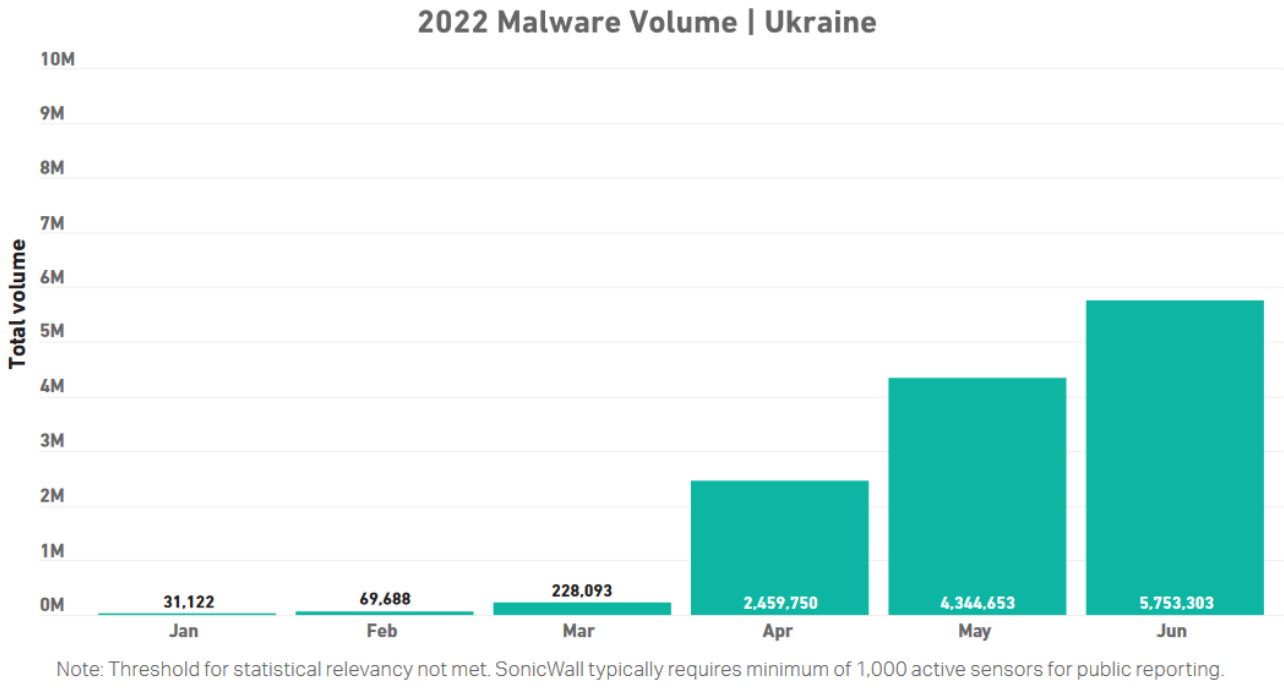
A utilização tem sido tão eficaz, que tanto Ucrânia quanto a Rússia, estão desenvolvendo e até já empregando drones com comando por IA. A grande vantagem da utilização da IA é que o bloqueio dos drones não funciona, uma vez que identificado

o alvo não existe mais a necessidade de comunicação com a base ou com o operador (Zafra; Hunder; Rao; Kiyada, 2024).

A inteligência artificial está transformando o conflito moderno e estabelecendo uma nova frente de batalha, na qual a gestão estratégica da informação desempenha um papel central. Em um teatro de operações moderno, o fluxo massivo de dados gerados em espaços de tempos cada vez mais curtos superam a capacidade humana de processamento e análise. Nesse contexto, algoritmos avançados são essenciais para sintetizar informações e identificar padrões em tempo real, impactando diretamente o planejamento militar e as decisões estratégicas (Eugênio, 2023).

A guerra cibernética no conflito vem sendo empregada em larga escala pelos dois lados, o gráfico abaixo retrata a evolução dos ataques ocorridos na Ucrânia após o início da invasão russa.

Figura 3: Aumento de ataques Malware a Ucrânia



Fonte: Relatório, 2022

Desde o início da invasão territorial em 2022, podemos destacar alguns ataques cibernéticos que marcaram o conflito:

a. Ataque ao KA-SAT (fevereiro de 2022): logo no início da invasão, hackers associados à Rússia realizaram um ataque cibernético a uma rede de satélites KA-SAT da Viasat. O ataque interrompeu as comunicações militares e civis da

Ucrânia, além de deixar sem acesso à internet milhares de pessoas na Europa (Presse, 2022);

b. Campanha de malware HermeticWiper (fevereiro de 2022): causou danos significativos a organizações ucranianas ao apagar totalmente os dados dos discos rígidos em sistemas Windows (Ucrânia, 2022);
c. Ataques DDoS (ataques de negação de serviço): os sites de várias agências governamentais ucranianas (incluindo os Ministérios das Relações Exteriores, Defesa e Assuntos Internos, o Serviço de Segurança e o Gabinete de Ministros) e dos dois maiores bancos estatais foram alvos de ataques DDoS (Efe, 2022);
d. Phishing ataque: o grupo de hackers, conhecidos com unidade APT28 (FancyBear), realizaram campanhas de phishing para coletar informações e espionar diplomatas e autoridades ucranianas (Dave, 2022); e
e. Defesa cibernética ucraniana e contra-ataques: a Ucrânia criou, em março de 2022, o *IT Army of Ukraine*, visando formar uma brigada de hackers voluntários em prol das forças armadas. Com o apoio de aliados internacionais, o exército digital ucraniano mobilizou em alguns dias cerca de 200 mil "hacktivistas" do mundo inteiro (Desaunay, 2023).

A guerra entre Ucrânia e Rússia, marcada por intensos ataques cibernéticos e a crescente sofisticação das ferramentas de inteligência artificial, demonstram a urgência de desenvolver sistemas de cibersegurança avançados. O volume exponencial de dados e a variedade de ameaças digitais exigem soluções robustas, capazes de detectar e neutralizar ataques com rapidez e precisão. A inteligência artificial emerge como uma ferramenta fundamental nesse contexto, permitindo a criação de sistemas de defesa proativos e adaptáveis.

2.2.2 utilização da IA na cibernética no conflito Israel x Hamas

O conflito em andamento entre Israel e o Hamas desencadeou um considerável aumento dos ataques cibernéticos, que continuam a se intensificar à medida que a guerra se prolonga, segundo dados da Check Point Software Technologies. De acordo com o levantamento de autoria dessa empresa israelense, houve um aumento de aproximadamente 20% nos ataques cibernéticos a Israel durante a guerra, incluindo mais de 50% quando se trata de ataques ao setor governamental (Brito, 2018).

A guerra teve início no dia 07 de outubro de 2023, e à medida que o confronto se desenvolve, os ataques cibernéticos se intensificam. Foi registrado um aumento significativo na frequência e sofisticação dos ataques cibernéticos. Embora inicialmente as ações fossem focadas em ataques distribuídos de negação de serviço, mais conhecidos como ataques DDoS *(Distributed Denial of Service - DDoS)* e desfigurações, isso está mudando (Brito, 2018).

O foco tem se direcionado para as organizações públicas e empresas que trabalham para o governo Israelense, com o vazamento diários de grandes bancos de dados retirados dos sites de pelo menos uma entidade. Como exemplo, temos o ataque à empresa *Max Security* com base em Israel, que é uma companhia de renome mundial especializada em soluções de segurança e gestão de riscos (Brito, 2018).

A contrapartida de Israel se deu com o aumento de investimentos na área cibernética, além da realização de ataques às redes de comunicação do Hamas. Os ataques contra sites palestinos, embora menos frequentes, foram por vezes mais graves, como por exemplo um ciberataque contra a *AlfaNet*, um provedor palestino de acesso à Internet com sede na Faixa de Gaza, atribuído ao grupo *Indian Cyber Force* (Ciberespaço, 2023).

Cabe salientar que uma das características mais notáveis do espaço cibernético é a possibilidade de anonimato, que torna difícil identificar o autor de uma ação. As identidades podem ser facilmente ocultadas ou trocadas, permitindo que a autoria de um ataque possa estar localizado em qualquer lugar do mundo. Essa característica é crucial para as operações de exploração realizadas antes do conflito. (Nunes, 2023).

Israel vem investindo em larga escala no desenvolvimento de IA. Em 2021, o país registrou um investimento massivo de US$ 2,41 bilhões em IA, quase dobrando o valor do ano anterior. Esse crescimento coloca o país à frente das principais potências de tecnologia no que diz respeito ao crescimento de investimentos no setor (Bodra, 2023).

Com o uso da IA Israel conseguiu, por exemplo: mapear a vasta rede de túneis subterrâneos do Hamas em Gaza aumentando a efetividade dos ataques e reduzindo as mortes de civis. Conforme informações obtidas com oficiais israelenses, o exército do país está utilizando um banco de dados alimentado por IA que já identificou 37 mil potenciais terroristas (Lorenzo, 2024).

2.3 DESENVOLVIMENTO DE IA PELAS FORÇAS ARMADAS

O combate moderno vem direcionando as grandes potências para desenvolver IA cada vez mais completas.

Nos EUA, um bom exemplo é o Projeto Maven, iniciado em 2017 em parceria com o Google, que tem como objetivo analisar imagens de drones usando IA para identificar alvos e permitir que militares revisem as imagens mais rapidamente. O projeto evoluiu para incorporar dados de radar e sensores infravermelhos e continua sendo aprimorado por empresas como Amazon e Microsoft, mesmo após a saída do Google em 2019. A Agência Nacional de Inteligência Geoespacial (NGA) é agora responsável pelo desenvolvimento do Maven, que se concentra em expandir a coleta de dados e melhorar a precisão na identificação de alvos no campo de batalha (Unzelte, 2024).

A OTAN discute a crescente militarização da inteligência artificial (IA), destacando a sua importância na competição global por hegemonia. A IA, especialmente em sistemas de armamento autônomo, traz benefícios e desafios, como questões éticas. O futuro da IA na segurança nacional promete inovações significativas, mas também requer vigilância (Sabino, 2022).

Da mesma forma que a proliferação de armas nucleares levanta sérias preocupações globais, o desenvolvimento de inteligência artificial para fins militares também gera inquietação. Um projeto apoiado por 60 países para a regulamentação do uso de inteligência artificial nas forças armadas foi anunciado durante uma conferência em Washington (Lee, 2024).

A iniciativa visa estabelecer diretrizes éticas e operacionais para o emprego responsável da IA no contexto militar. No entanto, a China optou por não participar, alegando que o projeto poderia intensificar a corrida armamentista global. Essa decisão ressalta as tensões internacionais em torno do uso de tecnologias emergentes para fins bélicos. (Lee, 2024).

Com base nos fatos apresentados, é evidente que a guerra cibernética, com a utilização de inteligência artificial, é uma realidade. Os países que desenvolverem suas soluções primeiro serão os líderes nesse campo, enquanto aqueles que ficarem dependentes terão que lidar com restrições futuras.

2.4 BRASIL NA CIBERNÉTICA E IA

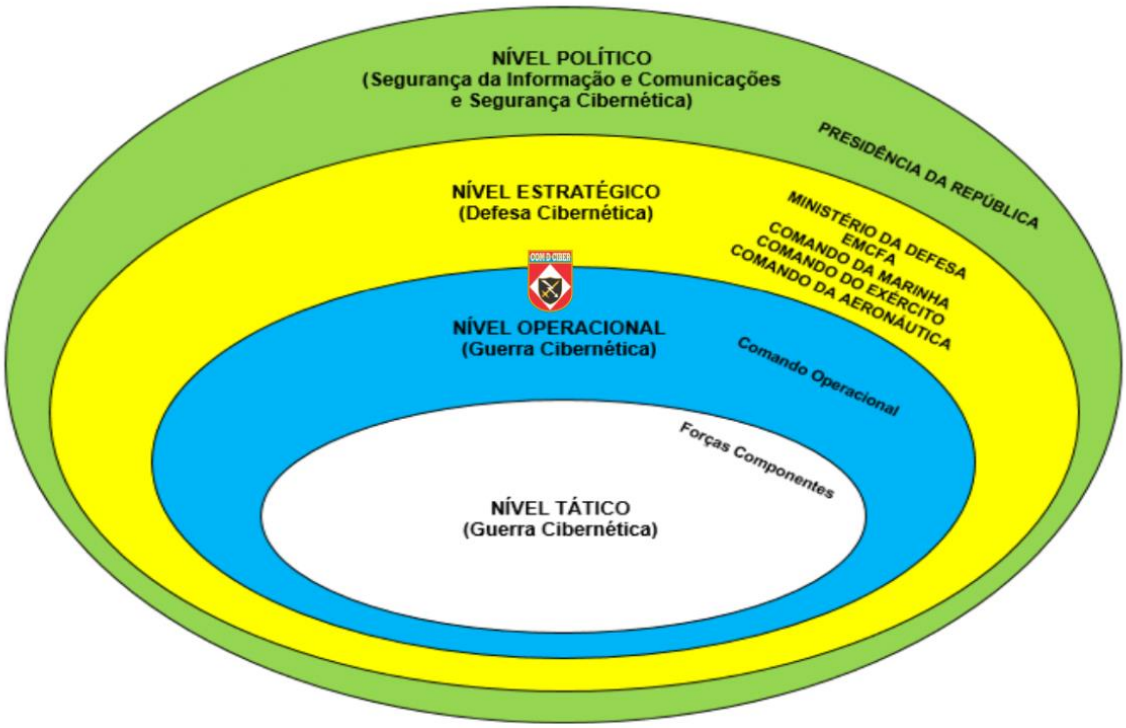
O Livro Branco da Defesa Nacional do Brasil, atualizado em 2020, classifica o setor cibernético como estratégico. Essa atualização enfatiza a importância da cibersegurança para a proteção das infraestruturas críticas do país e a necessidade de desenvolver políticas que integrem tecnologias digitais na defesa nacional. Segue abaixo trecho do livro (Brasil, 2020):

> "A possibilidade de o País sofrer um ataque cibernético de origens das mais diversas e de difícil identificação, que poderão causar danos consideráveis a estruturas estratégicas ou mesmo a outros setores de importâncias vitais para a nação brasileira, faz com que a Defesa Cibernética passe a ter importância fundamental para a Defesa Nacional."

Ainda em 2020, foi lançada a Estratégia Nacional de Segurança Cibernética. Neste documento existem várias referências ao uso de IA, inclusive pautando como essencial que o Brasil participe de iniciativas neste campo (Brasil, 2023b).

O Gabinete de Segurança Institucional (GSI) tem como parte de suas atribuições coordenar políticas públicas de segurança da informação e cibernética, no âmbito da administração pública federal (Brasil, 2023a).

Figura 4: Níveis da segurança cibernética (modelo cebola)



Fonte: Marra, 2018

O Comando de Defesa Cibernética (ComDCiber), vinculado ao Exército Brasileiro, tem como missão coordenar e integrar as atividades de defesa cibernética no âmbito do Ministério da Defesa (MD). Seu objetivo é consolidar as iniciativas no setor cibernético, dotando a Defesa Nacional com a infraestrutura e os recursos necessários para realizar um amplo espectro de ações cibernéticas. Essas ações visam proteger e defender os ativos de informação tanto do Ministério da Defesa quanto das Forças Armadas (FA), garantindo a segurança e resiliência cibernética do país (Marra, 2018).

Atualmente, o Brasil possui diversas iniciativas voltadas para o desenvolvimento de tecnologias de inteligência artificial (IA), mas ainda não alcançou um domínio abrangente nessa área (Brandão, 2024).

O país não pode se permitir ser apenas um consumidor de soluções em inteligência artificial desenvolvidas no exterior. A dependência de tecnologias e serviços de outros países e grandes empresas pode comprometer tanto a segurança e a soberania nacional quanto a competitividade das empresas brasileiras, tanto no mercado interno quanto no externo (Brandão, 2024).

A Inteligência Artificial (IA) tem se tornado um campo de pesquisa militar cada vez mais relevante, evidenciado pelos significativos investimentos realizados por potências militares como EUA, Rússia e China nos últimos anos. A implementação de IA pode aumentar a velocidade do processo decisório, superando as capacidades humanas (Althoff, 2022).

Na guerra do futuro, a liderança que não contar com IA, ou que utilizar tecnologias inferiores às de seus adversários, enfrentará desvantagens significativas. Portanto, é crucial que o Brasil invista recursos não apenas para adquirir essa tecnologia, mas também para garantir sua autonomia e independência em relação a outros países (Althoff, 2022).

2.5 POSSIBILIDADE DE DESENVOLVIMENTO DE IA NA DEFESA CIBERNÉTICA

Os conflitos contemporâneos têm evidenciado, cada vez mais, que a sinergia resultante do emprego conjunto das Forças Armadas, caracterizada pela interoperabilidade, é fundamental para obter o máximo rendimento da expressão militar do Poder Nacional (Brasil, 2020).

Nesse sentido, a concepção de emprego conjunto implica a compreensão, em seus aspectos gerais, de interesses comuns, de maneira que a interoperabilidade pode ser alcançada. Isso permite a aplicação adequada da expressão militar do Poder Nacional na busca de soluções rápidas e eficazes para os conflitos (Brasil, 2020).

Em um cenário cibernético em constante evolução, a capacidade de adaptação proporcionada pela tecnologia de IA, assegura uma defesa robusta e ágil contra invasões às infraestruturas críticas do país e suas aplicações militares (Moraes, 2023).

Atualmente, o Brasil enfrenta uma lacuna tecnológica em relação às grandes potências no campo da cibersegurança. A crescente relevância do ambiente cibernético será fundamental nos conflitos do futuro. O trabalho de coordenação de interagências e a atuação conjunta/unificada, será fundamental para seleção de tecnologias prioritárias capazes de suprir Forças Armadas, inteligência, Forças de Segurança e agências civis (Medeiros Filho; Lima, 2019).

O desafio de vencer este abismo tecnológico e dispor de uma IA que pode assegurar uma defesa cibernética, contribuindo para a manutenção da soberania do país, somente será viável com a junção dos esforços de vários setores da sociedade. No caso específico de pesquisa e desenvolvimento (P&D), a Tríplice Hélice é uma metodologia que pode viabilizar esse avanço.

A Tríplice Hélice é uma abordagem colaborativa que busca promover a inovação por meio da interação entre três pilares fundamentais: universidade ou academia, empresas e governo (Flores, 2023).

Considerando que o objetivo é desenvolver uma IA voltada para a ciberdefesa nacional, o órgão governamental mais adequado para liderar esse projeto é o Ministério da Defesa (MD). O MD, com o intuito de fortalecer a iniciativa, por meio do Estado-Maior Conjunto das Forças Armadas (EMCFA), deve promover a colaboração integrada entre as três Forças Armadas (FA), garantindo um esforço coordenado e eficaz na criação e implementação da tecnologia.

A proposta de criação de um Comando Conjunto de Inteligência Artificial (CCIA) visa facilitar a interação e otimizar a união de esforços das três Forças. Esse comando permitirá que as FA trabalhem de forma colaborativa e coordenada, com cada uma designando seus representantes para contribuir no desenvolvimento da IA, garantindo que suas respectivas necessidades e *expertise* sejam integradas no projeto.

Um segundo eixo de atuação será responsável por integrar os esforços na vertente acadêmica, tendo como principais pilares o Instituto Militar de Engenharia (IME), o Instituto Tecnológico de Aeronáutica (ITA) e instituições civis de ensino superior, que participarão por meio de convênios. Essas entidades serão responsáveis pela pesquisa e inovação no desenvolvimento da IA.

Por fim, o Comando Conjunto de Inteligência Artificial será encarregado de fomentar iniciativas tecnológicas junto ao setor empresarial brasileiro, visando o desenvolvimento completo e sustentável da ferramenta de IA.

O Ministério da Defesa apoiará as iniciativas por meio de recursos orçamentários, com a contrapartida de que as tecnologias desenvolvidas sejam empregadas, também, para a defesa nacional, assegurando a soberania e a segurança do país.

3 CONSIDERAÇÕES FINAIS

Assim como a proliferação de armas nucleares gera sérias preocupações globais, o desenvolvimento de inteligência artificial para fins militares também provoca inquietação.

Para garantir a plena soberania de um país, é essencial assegurar alguns aspectos fundamentais e tradicionais, como: soberania territorial, autonomia política, independência econômica, soberania alimentar e energética, força militar e defesa, controle sobre a infraestrutura crítica, preservação da identidade cultural e dos valores nacionais, diplomacia, participação em organizações internacionais e controle sobre a moeda e as políticas monetárias.

O Brasil controla essas áreas tradicionais, mas com o avanço da tecnologia da informação, novos fatores emergem, como a independência tecnológica, a inovação, a soberania digital e a proteção de dados.

Nessas áreas, o país ainda tem muito a progredir. Com o avanço tecnológico, a capacidade de proteger dados sensíveis, garantir a cibersegurança e controlar a infraestrutura digital tornou-se de suma importância. A dependência de serviços estrangeiros pode expor o Brasil a riscos de espionagem ou manipulação externa, comprometendo sua soberania.

A ferramenta que vem ganhando destaque e promete revolucionar o combate moderno é a Inteligência Artificial (IA). Ao permitir o processamento rápido e eficiente de grandes volumes de dados, a IA está transformando a forma como as decisões são

tomadas em tempo real nos campos de batalha. Sua capacidade de analisar informações complexas, identificar padrões e realizar tarefas automatizadas, que antes dependiam exclusivamente de intervenção humana, oferece vantagens estratégicas significativas.

No contexto militar, a IA pode ser aplicada em diversas frentes, como na operação de drones autônomos, na análise de inteligência cibernética e na defesa contra-ataques digitais. Além disso, sistemas de armamentos inteligentes, coordenados por IA, podem ser mais precisos e eficientes, minimizando danos colaterais e melhorando a eficiência das operações militares. Países que investirem em IA para fins de defesa estarão à frente na corrida tecnológica, consolidando sua posição no cenário global.

Essa revolução tecnológica está mudando as regras dos conflitos modernos, onde a velocidade da informação e a capacidade de adaptação em tempo real são fatores decisivos. A inteligência artificial, portanto, não só promete modernizar o combate, mas também redefinir o conceito de segurança nacional e defesa cibernética, sendo um recurso indispensável para as nações que buscam garantir sua soberania no futuro.

Para vencer essa lacuna tecnológica na área de defesa cibernética e inteligência artificial, o Brasil deve aproveitar, de forma colaborativa, as capacidades técnicas e científicas já disponíveis nas Forças Armadas.

Outro fator que justifica a ação conjunta das Forças Armadas é a limitação orçamentária para o desenvolvimento de tecnologias. Com as três Forças trabalhando em conjunto, haverá uma economia significativa de recursos.

Nesse contexto, a participação do Ministério da Defesa como agente catalisador para o desenvolvimento de projeto de aplicação da inteligência artificial, no meio militar, é fundamental para garantir a soberania do Estado brasileiro frente às crescentes ameaças decorrentes do uso da IA.

Somando os esforços das Forças Armadas e centralizando suas capacidades intelectuais e recursos, será possível envolver outros setores do governo federal e fomentar parcerias com empresas brasileiras.

Para concretizar essa estratégia, a proposta de criação de um Comando Conjunto de Inteligência Artificial (CCIA), vinculado diretamente ao EMCFA/MD, será fundamental. Esse comando terá a responsabilidade de coordenar e integrar as iniciativas de desenvolvimento de IA voltadas para a defesa, garantindo que o Brasil

avance de forma soberana e eficiente na proteção de suas infraestruturas críticas e no fortalecimento de sua posição tecnológica e militar no cenário global.

O trabalho do CCIA será conduzido com a metodologia da Tríplice Hélice, dessa forma a estrutura do Comando Conjunto de Inteligência Artificial deverá ter pelo menos três divisões: a governamental, a acadêmica e a empresarial.

A divisão governamental ficará encarregada de estabelecer a conexão com as Forças Armadas, identificando suas necessidades e áreas de especialização.

A divisão acadêmica será responsável por firmar convênios e selecionar pesquisas nas áreas de interesse, em colaboração com o Instituto Militar de Engenharia (IME), o Instituto Tecnológico de Aeronáutica (ITA) e universidades civis.

Por sua vez, a divisão empresarial terá como função promover o desenvolvimento abrangente e sustentável da ferramenta de Inteligência Artificial, em parceria com o setor empresarial brasileiro.

A proposta de criação de um Comando Conjunto de Inteligência Artificial, tem por objetivo viabilizar o avanço da IA na defesa cibernética, aumentando a capacidade de defesa do país, viabilizando soluções em tempo real, melhorando a detecção de ameaças e a resposta a incidentes, o que fortalece a soberania em um ambiente digital. Também permitirá atualizar os processos de análise de dados e tomada de decisão, melhorando a eficiência das operações militares e da defesa da nação, possibilitando o equilíbrio do poder entre países e oferecendo vantagem estratégica

Em suma, o Brasil poderá desenvolver uma tecnologia de inteligência artificial para a defesa, totalmente nacional e segura, superando os riscos associados à importação de soluções estrangeiras, que raramente oferecem controle completo ou transferência total de tecnologia.

REFERÊNCIAS

ALTHOFF, Paulo Eduardo. **Inteligência Artificial e o futuro do comando e controle.** 2022. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) - Escola de Aperfeiçoamento de Oficiais do Exército, Rio de Janeiro, 2022.

ANDRADE, Rodrigo de Oliveira. O universo expandido da inteligência artificial. **Revista Pesquisa FAPESP**, São Paulo, 2023. Disponível em: https://revistapesquisa.fapesp.br/o-universo-expandido-da-inteligencia-artificial/. Acesso em: 13 out. 2024.

BELANDI, Caio. A População do Brasil chega a 212,6 milhões de habitantes, aponta o IBGE. **Agência IBGE Notícias**, 29 ago. 2024. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/41111-populacao-estimada-do-pais-chega-a-212-6-milhoes-de-habitantes-em-2024#:~:text=O%20IBGE%20divulga%20hoje%20(29,212%2C6%20milh%C3%B5es%20de%20habitantes. Acesso em: 13 out. 2024.

BODRA, Gustavo. Qual país será o próximo líder da revolução da Inteligência Artificial. **Startse**, 4 ago. 2023. Disponível em: https://www.startse.com/artigos/israel-lider-em-ia/. Acesso em: 21 out. 2024.

BRANDÃO, Rodrigo. O cenário atual de desenvolvimento da Inteligência Artificial no Brasil. **Panorama Setorial da Internet**, v. 16, n. 1, abr. 2024. Disponível em: https://ppl-ai-file-upload.s3.amazonaws.com/web/direct-files/34500926/82803b10-7e85-4e4c-86c0-1db8997856e2/psi-ano-xvi-n-1-desenvolvimento-ia-brasil.pdf. Acesso em: 13 out. 2024.

BRASIL. Decreto nº 11.676, de 30 de agosto de 2023. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão, das Funções de Confiança e das Gratificações do Gabinete de Segurança Institucional da Presidência da República, e remaneja e transforma cargos em comissão, funções de confiança e gratificações. **Diário Oficial da União**, Brasília, DF, 30 ago. 2023a. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-11.676-de-30-de-agosto-de-2023-506996152. Acesso em: 13 out. 2024.

BRASIL. Ministério da Defesa. **Livro Branco da Defesa Nacional**. Brasília, DF: MD, 2020. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/publicacoes/livro-branco-da-defesa-nacional-2020. Acesso em: 03 out. 2024.

BRASIL. Ministério da Defesa. **MD31-M-07: Doutrina de Defesa Cibernética**. 2. ed. Brasília, DF: MD, 2023b. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.gov.br/defesa/pt-br/assuntos/estado-maior-conjunto-das-forcas-armadas/doutrina-militar/publicacoes-1/publicacoes/MD31M07DoutrinaMilitardeDefesaCiberntica2Edio2023.pdf. Acesso em: 13 out. 2024.

BRITO, Paulo. Ciberataques crescendo com intensificação da guerra Israel-Hamas. **CISO Advisor**, 23 out. 2018. Disponível em: https://www.cisoadvisor.com.br/ciberataques-crescem-com-intensificacao-da-guerra-israel-hamas/. Acesso em: 3 out. 2024.

CAMPOS, Matheus. Os 20 maiores países do mundo. **Mundo Educação**, 2024. Disponível em: https://mundoeducacao.uol.com.br/geografia/os-maiores-paises-mundo.htm. Acesso em: 13 out. 2024.

CIBERESPAÇO, outro campo de batalha entre Israel e Hamas. **Exame**, 13 out. 2023. Disponível em: https://exame.com/tecnologia/ciberespaco-outro-campo-de-batalha-entre-israel-e-hamas/ . Acesso: 5 out. 2024.

DAVE, Paresh. Hackers da Rússia e da Bielorrússia atacam a Ucrânia com phishing, diz Google. **Agência Brasil**, 04 mar. 2022. Disponível em: https://agenciabrasil.ebc.com.br/internacional/noticia/2022-03/hackers-da-russia-e-de-belarus-atacam-ucrania-com-phishing-diz-google. Acesso em: 3 out. 2024.

DÉBORA. O papel da inteligência artificial. **DIO**, 08 set. 2023. Disponível em: https://www.dio.me/articles/o-papel-da-inteligencia-artificial-na-ciberseguranca. Acesso em: 2 out. 2024.

DESAUNAY, Dominique. A Ucrânia quer integrar hackers voluntários em seu Exército. **G1**, 05 abr. 2023. Mundo. Disponível em: https://g1.globo.com/mundo/ucrania-russia/noticia/2023/04/05/ucrania-quer-integrar-hackers-voluntarios-em-seu-exercito.ghtml. Acesso em: 3 out. 2024.

EFE, A. Ucrânia denuncia ciberataque contra Ministério da Defesa e bancos. **Gazeta do Povo**, 2022. Disponível em: https://www.gazetadopovo.com.br/mundo/ucrania-denuncia-ciberataque-contra-ministerio-da-defesa-e-bancos/. Acesso em: 21 out. 2024.

EUGÉNIO, António. Soberania tecnológica: o exemplo da Ucrânia. IDN **Nação e Defesa**, n. 165, 2023. Disponível em: revistas.rcaap.pt/nacao/article/view/35443. Acesso em: 3 out. 2024.

FIGUEIREDO, Ana Luiza. 6 meses de ChatGPT: o que mudou e o que está por vir. **Olhar Digital**. 30 mai. 2023. Disponível em: https://olhardigital.com.br/2023/05/30/pro/6-meses-de-chatgpt-o-que-mudou-e-o-que-esta-por-vir/

FLORES, Diego. O que é Tríplice Hélice. **Quikdev**, 11 maio 2023. Disponível em: https://quikdev.com.br/triplice-helice/ . Acesso em: 21 out. 2024.

GONCHARUK, Vitali. O uso da inteligência artificial na guerra e os riscos de um conflito nuclear. **Correio do Povo**, Porto Alegre, 10 abr. 2024. Disponível em: https://www.correiodopovo.com.br/jornal-com-tecnologia/o-uso-da-intelig%C3%AAncia-artificial-na-guerra-e-os-riscos-de-um-conflito-nuclear-1.1482889. Acesso em: 13 out. 2024.

LEE, Joyce. 60 países apoiam projeto para uso de IA nas forças armadas; China decide não participar. **CNN Brasil**, 04 abr. 2024. Disponível em: https://www.cnnbrasil.com.br/internacional/60-paises-apoiam-projeto-para-uso-de-ia-nas-forcas-armadas-china-decide-nao-participar/. Acesso em: 3 out. 2024.

LORENZO, Alessandro Di. IA usada por Israel acordos 37 mil alvos do Hamas em Gaza. **Olhar Digital**, 04 abr. 2024. Disponível em: https://olhardigital.com.br/2024/04/04/pro/ia-usada-por-israel-identificou-37-mil-alvos-do-hamas-em-gaza/. Acesso em: 3 out. 2024.

MARRA, Mauro Fernando Costa. Programa da Defesa Cibernética na Defesa Nacional. **Palestra apresentada no CADN**, 2018. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/ensino_e_pesquisa/defesa_academia/cadn/palestra_cadn_xi/xv_cadn/programaa_daa_defesaa_ciberneticaa_naa_defesaa_nacional.pdf. Acesso em: 13 out. 2024.

MCCARTHY, J.;MINSKY, M. L.; ROCHESTER, N. e SHANNON, C. E. (2006). **A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence**. 1955. AI Magazine, 27(4), 12. Disponível em: https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/1904. Acesso em: 13 out. 2024.

MEDEIROS FILHO, Oscar; LIMA, Rafael Camargo. **Guerra do Futuro**: sínteses e recomendações. Brasília, DF: Centro de Estudos Estratégicos do Exército, 2019.

MORAES, Leonardo Bastos. **O papel da inteligência artificial na gestão de riscos cibernéticos em apoio ao plano de respostas a incidentes em ambientes em nuvem para aplicações militares**. 2023. Trabalho de Conclusão de Curso (Especialização em Segurança e Defesa Cibernética) - Escola Superior de Guerra, Rio de Janeiro, 2023.

OCDE. Artificial Intelligence in Society. **OECD Publishing**. 2019. Disponível em: https://www.oecd-ilibrary.org/science-and-technology/artificial-intelligence-in-society_eedfee77-en. Acesso em: 23/09/24.

OLIVEIRA, CMG Márcio Rebello de. **As infraestruturas críticas nacionais ante às ameaças cibernéticas**: análise comparativa das governanças cibernéticas do Brasil e do Reino Unido, com foco nas infraestruturas críticas marítimas. 2022. Dissertação (Curso de Política e Estratégia Marítimas) - Escola de Guerra Naval, Rio de Janeiro, 2022.

PRESSE, France. Ataque cibernético deixa milhares sem internet na Europa. **G1**, 04 mar. 2022. Tecnologia. Disponível em:

https://g1.globo.com/tecnologia/noticia/2022/03/04/ataque-cibernetico-deixa-milhares-sem-internet-na-europa.ghtml. Acesso em: 3 out. 2024.

RELATÓRIO de ameaças cibernéticas de 2022. **SonicWall**, 2022. Disponível em: https://www.sonicwall.com/resources/white-papers/executive-summary-2022-sonicwall-cyber-threat-report . Acesso em: 21 out. 2024.

ROSENBERG, Steve. Como dois anos de guerra na Ucrânia mudaram para a Rússia. **BBC Brasil**, 23 fev. 2024. Disponível em: https://www.bbc.com/portuguese/articles/cnlnngrzzzeo. Acesso em: 13 out. 2024.

SABINO, Sebastião. A OTAN e a Militarização da Inteligência Artificial. **Eurodefense**, 12 mai. 2022. Disponível em: https://eurodefense.pt/a-nato-e-a-militarizacao-da-inteligencia-artificial/. Acesso em: 14 out. 2024.

SPECTOR, Lee. **Evolution of artificial intelligence**. Sciencedirect, v. 170, p. 1251-1253, 2006.

TURING, A. M. **Computing Machinery and Intelligenc**e. Mind 49: 433-460, 1950.

UCRÂNIA sofre ciberataques do malware HermeticWiper. **Tiinside**, 24 fev. 2022. Disponível em: https://tiinside.com.br/24/02/2022/ucrania-sofre-ciberataques-do-malware-hermeticwiper/. Acesso em: 3 out. 2024.

UNZELTE, Carolina. O que se sabe sobre o Projeto Maven, o programa militar de IA dos EUA. **Exame**, 04 abr. 2024. Disponível em: https://exame.com/inteligencia-artificial/o-que-se-sabe-sobre-o-projeto-maven-o-programa-militar-de-ia-dos-eua/. Acesso em: 3 out. 2024.

ZAFRA, Mariano; HUNDER, Max; RAO, Anurag; KIYADA, Sudev. Crise na Ucrânia: drones. **Reuters**, 26 mar. 2024. Disponível em: https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/ . Acesso em: 21 out. 2024.