ESCOLA DE GUERRA NAVAL

CL PLÍNIO DA SILVA BECKER

NOVAS TECNOLOGIAS APLICADAS EM PROCESSOS DECISÓRIOS MILITARES

Confiabilidade, Riscos e Incertezas

Rio de Janeiro

2024

CL PLÍNIO DA SILVA BECKER

NOVAS TECNOLOGIAS APLICADAS EM PROCESSOS DECISÓRIOS MILITARES

Confiabilidade, Riscos e Incertezas

Tese apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Política e Estratégia Marítimas.

Orientador: CMG (RM1) WALTER MAURÍCIO

Rio de Janeiro
Escola de Guerra Naval
2024

DECLARAÇÃO DA NÃO EXISTÊNCIA DE APROPRIAÇÃO INTELECTUAL IRREGULAR

Declaro que este trabalho acadêmico: a) corresponde ao resultado de investigação por mim desenvolvida, enquanto discente da Escola de Guerra Naval (EGN); b) é um trabalho original, ou seja, que não foi por mim anteriormente utilizado para fins acadêmicos ou quaisquer outros; c) é inédito, isto é, não foi ainda objeto de publicação; e d) é de minha integral e exclusiva autoria.

Declaro também que tenho ciência de que a utilização de ideias ou palavras de autoria de outrem, sem a devida identificação da fonte, e o uso de recursos de inteligência artificial no processo de escrita constituem grave falta ética, moral, legal e disciplinar. Ademais, assumo o compromisso de que este trabalho possa, a qualquer tempo, ser analisado para verificação de sua originalidade e ineditismo, por meio de ferramentas de detecção de similaridades ou por profissionais qualificados.

Os conceitos e ideias expressas neste trabalho acadêmico são de responsabilidade do Autor e não retratam qualquer orientação institucional da EGN ou da Marinha do Brasil.

gov.br
Documento assinado digitalmente
PLINIO DA SILVA BECKER
Data: 26/11/2024 20:12:12-0300
Verifique em https://validar.iti.gov.br

AGRADECIMENTOS

Em primeiro lugar, agradeço ao grande arquiteto por me proporcionar a saúde, serenidade, persistência e resiliência para superar os desafios e aproveitar as oportunidades desta jornada.

Aos meus familiares, em especial à minha esposa e filhas, pela compreensão de minhas ausências, encorajamento e apoio incondicional.

Ao meu orientador, Capitão de Mar e Guerra (RM1) Walter Maurício Costa de Miranda, pela disponibilidade, cordialidade e contribuições assertivas para a melhoria deste trabalho.

Aos instrutores da Escola de Guerra Naval, registro meu respeito e admiração pela abnegação, entusiasmo e nível dos conteúdos apresentados, que muito contribuíram para o meu aprimoramento profissional.

Aos meu novos amigos da turma do Curso de Política e Estratégia Marítimas (C-PEM) 2024, pelo convívio saudável, amigável e colaborativo.

Por fim, deixo meu reconhecimento ao Ajudante e ao Encarregado do C-PEM 2024 pelo apoio e profissionalismo demonstrados em todos os momentos.

RESUMO

Esta pesquisa tem por objetivo analisar os principais requisitos que sustentam a confiabilidade das arquiteturas de sistemas de apoio ao processo decisório militar que empregam novas tecnologias. Inicia com a abordagem do modelo do processo mental humano e das teorias clássicas da decisão, avançando para as capacidades das modernas ferramentas tecnológicas, destacando seu potencial de emprego em cenários complexos e dinâmicos, sujeitos a riscos e incertezas. Apresenta a evolução tecnológica que, impulsionada por avanços como o *Big Data* e a Inteligência Artificial, permite a integração e a análise de um grande volume de dados, fornecendo recomendações com alto nível de precisão, adaptativas e em tempo real, representando uma possibilidade de revolução nos assuntos militares, por meio da proposição de novas táticas e da ruptura de paradigmas estratégicos. Sob a perspectiva do emprego militar confiável de novas tecnologias em sistemas de apoio à decisão, esta pesquisa identifica e explica os principais requisitos de confiabilidade, denominados transparência algorítmica, explicabilidade, interoperabilidade, robustez, redundância e responsabilidade. As análises individualizadas e pormenorizadas de cada requisito identificaram profundas relações de interdependência e colaboração entre os mesmos e que um simples *trade-off* não é uma solução aplicável a este tipo de sistema. O trabalho também conclui que é essencial que sistemas de apoio à decisão militares sejam desenvolvidos em conjunto pelas Forças Armadas, sem que represente perda de poder de decisão ou de autonomia, mas uma evolução da cultura organizacional. O principal resultado da pesquisa está na proposição de soluções técnicas e estratégicas que contribuirão para orientar o desenvolvimento de diretrizes fundamentais para garantir confiabilidade operacional e segurança algorítmica em sistemas de apoio à decisão militar.

Palavras-chave: Confiabilidade. Explicabilidade. Incerteza. Inteligência artificial. Interoperabilidade. Processo decisório. Redundância. Responsabilidade. Risco. Robustez. Sistema de apoio à decisão. Transparência algorítmica.

ABSTRACT

NEW TECHNOLOGIES APPLIED IN MILITARY DECISION-MAKING PROCESSES
Reliability, Risks, and Uncertainties

This research aims to analyze the main requirements that underpin the reliability of architectures of military decision-making support systems that employ new technologies. It begins by addressing the model of the human mental process and classical decision theories, advancing towards the capabilities of modern technological tools, highlighting their potential use in complex and dynamic scenarios subject to risks and uncertainties. The study presents the technological evolution driven by advancements such as Big Data and Artificial Intelligence, which allows the integration and analysis of a large volume of data, providing highly accurate, adaptive, and real-time recommendations. This represents the possibility of a revolution in military affairs through the proposition of new tactics and the disruption of strategic paradigms. From the perspective of reliable military use of new technologies in decision support systems, this research identifies and examines the main reliability requirements, known as algorithmic transparency, explainability, interoperability, robustness, redundancy, and accountability. The detailed and individualized analyses of each requirement revealed deep interdependencies and collaborative relationships among them, indicating that a simple trade-off is not an applicable solution for this type of system. The study also concludes that it is essential for military decision support systems to be developed jointly by the Armed Forces, without compromising decision-making power or autonomy, but rather representing an evolution of organizational culture. The main outcome of the research is the proposition of technical and strategic solutions that will contribute to guiding the development of fundamental guidelines to ensure operational reliability and algorithmic security in military decision support systems.

Keywords: Reliability. Explainability. Uncertainty. Artificial Intelligence. Interoperability. Decision-making process. Redundancy. Accountability. Risk. Robustness. Decision support system. Algorithmic transparency.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

API	*Application Programming Interfaces*
C2	Comando e Controle
CND	Capacidades Nacionais de Defesa
CPC	Comparação de Poderes de Combate
DIH	Direito Internacional Humanitário
DL	*Deep Learning*
DoD	*Department of Defense*
EB	Exército Brasileiro
EGN	Escola de Guerra Naval
ENAP	Escola Nacional de Administração Pública
END	Estratégia Nacional de Defesa
FAB	Força Aérea Brasileira
IA	Inteligência Artificial
IoT	*Internet of Things*
LAWS	*Lethal Autonomous Weapons Systems*
MB	Marinha do Brasil
MCTI	Ministério da Ciência, Tecnologia e Inovação
MD	Ministério da Defesa
ML	*Machine Learning*
NLP	*Natural Language Processing*
PBIA	Plano Brasileiro de Inteligência Artificial
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
PL	Projeto de Lei
SI	Sistema de Informação
SIGMA	Sistema de Gerenciamento de Movimentos Aéreos
SNT	Sistemas Não-Tripulados
TI	Tecnologia da Informação
TNP	Tratado de Não-Proliferação de Armas Nucleares
USS	*United States Ship*

SUMÁRIO

1 INTRODUÇÃO

No início do século XIX, na obra intitulada “Da Guerra”, Carl von Clausewitz descreveu o dinamismo e a multiplicidade de variáveis como características inerentes aos conflitos bélicos, destacando a complexidade, os riscos e as incertezas desses cenários. Afirmava ainda que, durante a progressão dos eventos, ocorriam dificuldades práticas e imprevistas, denominadas “fricção”, que mudavam o curso do planejamento inicial e influenciavam continuamente o processo de tomada de decisão dos Comandantes.

Durante a sexagésima quinta sessão anual da Assembleia Parlamentar da OTAN, ocorrida em 2019, foram apresentadas as implicações do emprego da inteligência artificial (IA) para as Forças Armadas (FA), destacando as principais oportunidades, desafios e incertezas para defesa e segurança, realizando abordagens sobre sistemas de apoio à gestão da informação, ao processo de tomada de decisão, sistemas autônomos, desafios técnicos e não técnicos e algumas implicações estratégicas potenciais. Abordou, ainda, o dinamismo do ambiente de informações, a sua tendência ao crescimento exponencial e a necessidade de processamento adequado.

A Estratégia Nacional de Defesa americana (*National Defense Strategy*, 2022) ressalta a importância do investimento em pesquisa e desenvolvimento de novas tecnologias, citando-a como a base da vantagem militar americana. Neste aspecto, apresenta diretamente o emprego da IA confiável e sistemas autônomos como capacidades militares relevantes, dado que as operações conjuntas dependem cada vez mais de tecnologias baseadas em informações e da integração de diversas fontes de dados.

No Brasil, a Estratégia Nacional de Defesa (END), no capítulo que aborda as Capacidades Nacionais de Defesa (CND), apresenta a Capacidade de Gestão da Informação como forma de “garantir a obtenção, a produção e a difusão dos conhecimentos necessários ao processo decisório e a coordenação e controle dos meios de que dispõe a Nação, proporcionando o acesso à Inteligência aos tomadores de decisão, em todos os níveis. Essa capacidade proporciona condições para a ação preventiva do poder público e contribui para a eficácia dos meios operativos das Forças Armadas” (BRASIL, 2020).

Considerando a gestão da informação como uma metodologia sistemática de processamento de um conjunto de dados, os quais devem estar disponíveis de forma rápida, segura e eficaz, associadas aos planos da complexidade multidimensional, das incertezas, do dinamismo e da fricção citadas por Clausewitz, o processamento puramente dependente das capacidades do cérebro humano torna-se insuficiente e limitado. Com isso, o emprego de ferramentas que sejam capazes de coletar, discriminar, categorizar, analisar, identificar padrões estatísticos, observar tendências, correlacionar e, inclusive, propor alternativas, têm se mostrado como determinantes para a visão gerencial holística e o processo decisório assertivo.

O progresso exponencial das aplicações tecnológicas observado nos últimos anos deve-se a diversos fatores, especialmente devido ao aumento do desempenho da capacidade de processamento e da disponibilidade de grande volume de dados, por meio da internet, de estruturas de *Big Data* e desenvolvimento de técnicas de aprendizado de máquina e redes neurais profundas.

Uma potencialidade desdobrada da utilização de sistemas baseados em tecnologias associados ao processo decisório trata da possibilidade de contribuição para a redução de influência de algumas características inerentes ao modelo de raciocínio humano, tais como limitações de conhecimento, heurísticas, vieses cognitivos e emocionais. Ao utilizar ferramentas algorítmicas específicas e modelos estatísticos consolidados baseados em um amplo conjunto de dados empíricos, os decisores terão à disposição novas perspectivas para apoio à decisão com filtros para tais influências.

No entanto, não apenas o desempenho, caracterizado pela rapidez, eficiência e capacidade de processamento, mostra-se essencial para sistemas de apoio à decisão. Especialmente em contextos militares, as soluções devem integrar requisitos específicos de tolerância a falhas, segurança e resiliência, assegurando que o sistema não apenas opere rapidamente, mas também de forma confiável, traduzindo-se na necessidade de uma relação ponderada entre desempenho e confiabilidade.

Neste sentido, sendo a confiabilidade um dos pilares estruturais de sistemas, este trabalho terá como questão de pesquisa os principais requisitos de confiabilidade de sistemas de apoio à decisão que utilizam novas ferramentas tecnológicas, tendo como objeto de pesquisa os sistemas que operam em ambientes de risco e incerteza, caracterizados pelo emprego militar. Por conseguinte, terá como objetivo analisar os

principais requisitos que sustentam a confiabilidade das arquiteturas de sistemas de apoio ao processo decisório militar que empregam novas tecnologias.

Este trabalho justifica-se pela possibilidade de proporcionar contribuições estratégicas e técnicas para as FA no desenvolvimento de arquiteturas interoperáveis, precisas e confiáveis para emprego em sistemas de processos decisórios.

A metodologia adotada neste trabalho caracteriza-se como uma pesquisa descritiva ampla e multidisciplinar, por meio de uma revisão crítica e correlacional entre as teorias estudadas, permitindo a construção de uma análise dos requisitos de confiabilidade atinentes às características das novas tecnologias e de riscos e incertezas decorrentes do processo decisório militar.

Em atenção ao arcabouço conceitual necessário para fins de fundamentação teórica, foram utilizadas referências bibliográficas de variadas fontes de informação disponíveis, tais como livros, publicações científicas, documentos técnicos, manuais militares, artigos acadêmicos gerais e específicos, com destaque às teorias desenvolvidas por Daniel Kahneman, no que se refere ao processo decisório, e ao trabalho científico de Bo Li e outros, que apresentam conceitos sobre confiabilidade em IA.

Com efeito, para se atingir o objetivo geral, foi necessário o delineamento de um caminho sistemático, progressivo e com encadeamento lógico-construtivo constituído de objetivos específicos, definidos como a análise do processo decisório, o estudo das novas tecnologias e integração dos conceitos em sistemas de apoio à decisão militar. Assim, a estruturação deste trabalho foi concebida em 5 capítulos, abrangendo desde esta Introdução, em que foram abordadas as considerações gerais, até a Conclusão com a síntese de todo o estudo realizado.

No capítulo 2, adotando as principais teorias propostas por Daniel Kahneman, Amos Tversky e Thomas Bayes, além de metodologias consagradas de análise multicritério, serão apresentados os principais conceitos sobre o processo decisório racional, sendo abordadas questões relacionadas à dinâmica mental, às limitações e às influências inerentes ao decisor humano. A compreensão dos mecanismos do raciocínio humano, suas limitações e seus fatores de influência serão essenciais para fins de identificar as possibilidades de emprego das ferramentas de apoio à decisão.

O capítulo 3 apresentará as principais tecnologias atualmente disponíveis, abordando um breve histórico do seu desenvolvimento, suas expectativas, correlações, interdependências, formas de utilização e algumas limitações técnicas.

Neste contexto, serão ainda analisados conceitos sobre riscos, incerteza e confiabilidade.

Conhecidos os aspectos do raciocínio humano, as novas tecnologias disponíveis, as conceituações sobre riscos, incertezas e confiabilidade, o capítulo 4 discorrerá sobre o emprego militar e, sob esta perspectiva, analisará os requisitos de confiabilidade essenciais para sistemas de apoio à decisão, alcançando o objetivo e respondendo à questão de pesquisa.

O quinto e último capítulo apresentará uma conclusão do trabalho com uma síntese dos principais resultados obtidos no estudo.

A relevância deste trabalho consiste em sua contribuição para aumentar a qualidade e a segurança para o desenvolvimento e emprego de ferramentas tecnológicas de apoio ao processo de tomada de decisão nos mais altos níveis das FA, por meio de proposições de soluções teóricas aplicáveis aos sistemas de apoio à decisão militar em uso ou que venham a ser desenvolvidos.

Como ressalva, cumpre destacar que a ampla variedade de ferramentas tecnológicas disponíveis são partes integrantes e colaborativas do processo decisório e não devem substituir completamente o julgamento humano em decisões de alto nível, sendo necessário que os tomadores de decisão avaliem criticamente as informações recebidas, que considerem as diferentes perspectivas e ponderem, com base em suas próprias experiências, os potenciais impactos de suas escolhas.

2 O PROCESSO DECISÓRIO

Este capítulo apresentará as principais teorias relacionadas ao processo decisório, por meio da apresentação da dinâmica mental humana, as suas limitações e as influências inerentes ao decisor. Ao conhecê-las, poderão ser identificadas as capacidades humanas que podem ser potencializadas e, por outro lado, adotar mecanismos de correção de falhas intrínsecas, aspectos essenciais para fins de desenvolvimento, utilização e garantia da confiabilidade das novas ferramentas que podem ser empregadas em apoio à decisão e que serão apresentadas nos capítulos posteriores.

Covello e Munpower (1985 apud Navarro, 2009, p. 37) citam que, por volta de 3.200 a.C., no vale entre os rios Tigre e Eufrates, vivia um grupo chamado Asipu. Uma das principais funções dos membros do grupo era auxiliar pessoas que precisavam tomar decisões difíceis. Quando procurado, o Asipu identificava a dimensão do problema, as alternativas e as consequências de cada decisão. Assim, elaborava uma tabela, marcando os pontos positivos e negativos de cada uma delas, para indicar a melhor opção. Estima-se que este seja o primeiro registro histórico de uma metodologia para suporte ao processo decisório, segundo o qual estava estruturado na definição de critérios e em uma consulta a uma base de conhecimento e experiência centrada no ser humano.

A ação de decidir está presente na rotina diária das pessoas, organizações e, até, nos animais. Segundo Freitas e Kladis (1995), este ato ocorre nas mais variadas circunstâncias, idades e posições sociais dos indivíduos. A simples escolha de um programa de TV ou de um vestuário envolve um processo de tomada de decisão. Um predador que escolhe o caminho e o momento de atacar sua presa, está tomando uma decisão. Considerando uma grande organização ou o emprego militar, o número de variáveis envolvidas e suas interrelações aumentam expressivamente e, somadas à incerteza e ao risco, tornam o processo decisório uma atividade complexa, competitiva e dinâmica.

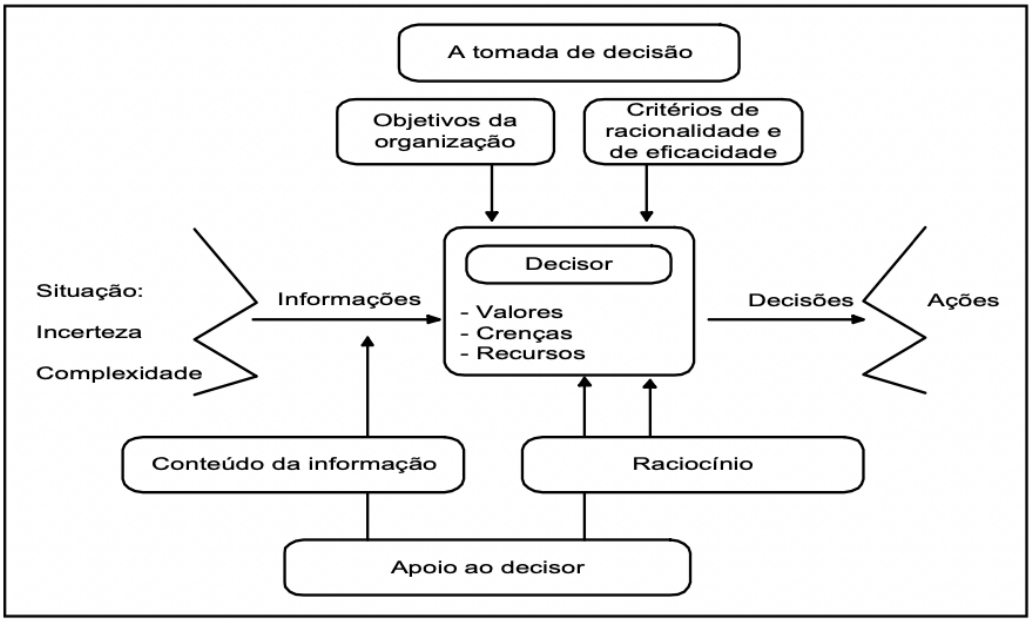
Na obra intitulada "*Administrative Behavior*", originalmente publicada em 1947, Herbert A. Simon realizou uma análise profunda sobre como os gestores e administradores resolvem problemas e tomam decisões em ambientes organizacionais complexos, impulsionando o desenvolvimento de teorias da decisão. Simon introduziu o conceito-chave da racionalidade limitada, em que os indivíduos

são incapazes de considerar todas as alternativas disponíveis devido às restrições cognitivas e de tempo. Ele argumentava que, em vez de maximizar resultados, os decisores frequentemente buscam soluções satisfatórias apenas o suficiente para resolver o problema dentro das limitações encontradas.

O processo decisório é o conjunto de etapas ou passos que uma pessoa ou organização segue para chegar a uma ação ou resultado. Envolve, de uma maneira simplificada, a identificação ou definição de um problema ou questão a ser resolvida, a análise de todos os conhecimentos anteriores relacionados ao tema, a síntese das suas interrelações, a geração de alternativas possíveis, a avaliação dessas alternativas, a escolha da melhor opção, a implementação, avaliação dos resultados obtidos.

A figura 1 apresenta o modelo esquemático da tomada de decisão proposto por Freitas (1993), apresentando as principais variáveis envolvidas e destacando o decisor como elemento central. Além isso, observa-se que o raciocínio é suportado por recursos de apoio ao decisor, os quais também são estruturantes para a geração de novas informações.

Figura 1 – A tomada de decisão



Fonte: Freitas, 1993

A busca pelo conhecimento da modelagem mental do processo decisório constitui-se em um desafiador campo de estudos multidisciplinar. A base de dados, os diferentes contextos e a percepção de possíveis consequências imediatas ou

futuras podem alterar significativamente o resultado. Assim, a decisão transcende o simples ato de escolher entre opções, pois o processo que a conduz, além do cenário em que está inserida, envolve domínios dos campos cognitivos e emocionais, podendo determinar o sucesso ou fracasso de uma organização.

2.1 PROCESSOS MENTAIS: O SISTEMA AUTOMÁTICO E O SISTEMA RACIONAL

A compreensão dos processos mentais e da cognição humana, incluindo habilidades como aprendizado, raciocínio lógico, tomada de decisão, reconhecimento de padrões, compreensão de linguagem natural e resolução de problemas complexos são ponto de partida para o desenvolvimento de algoritmos e sistemas que possam simular, replicar ou tomar decisões autônomas.

Daniel Kahneman (2012) apresentou um modelo de processo mental que define como as decisões são tomadas por meio da teorização da existência de dois sistemas mentais, denominados, de forma simplificada, como Sistema 1 e Sistema 2, que governam o pensamento humano e influenciam nas escolhas.

O Sistema 1, também conhecido como o "sistema automático", é responsável por executar processos cognitivos rápidos e intuitivos. Baseia-se em simplificações mentais que permitem respostas instantâneas a estímulos do ambiente. Este sistema é altamente eficiente em situações de perigo ou em atividades cotidianas, permitindo respostas automáticas. No entanto, possui propensão à heurísticas, vieses cognitivos e erros de julgamento que podem levar a decisões inadequadas, principalmente em situações complexas ou ambíguas.

O Sistema 2, por sua vez, é o "sistema racional" que opera de forma deliberada, analítica e consciente. Envolve processos mentais mais lentos, exigindo esforço cognitivo e atenção concentrada. Este sistema é acionado em situações que demandam análise crítica, cálculos complexos e tomadas de decisão ponderadas. Embora mais preciso e capaz de corrigir os vieses do Sistema 1, o Sistema 2 consome mais recursos mentais e pode levar à fadiga decisória, caso sobrecarregado.

Kahneman (2012) destaca a interação dinâmica entre os sistemas mentais, enfatizando que a maioria das decisões é influenciada pela interrelação entre o Sistema 1 e o Sistema 2. Enquanto o Sistema 1 fornece respostas rápidas e

automáticas, o Sistema 2 entra em ação para validar, corrigir e aprofundar essas respostas quando necessário. A capacidade de reconhecer quando cada sistema deve ser empregado é essencial para a tomada de decisões eficaz e consciente.

A compreensão do modelo de sistemas mentais de Kahneman tem implicações significativas em diversas áreas, permitindo o reconhecimento de padrões de pensamento e os vieses inerentes a cada sistema, indivíduos e organizações. Ao compreender tais características, poderão ser adotadas estratégias para mitigar erros de julgamento, promover a tomada de decisões mais acertadas e melhorar a eficácia na resolução de problemas complexos.

2.2 HEURÍSTICAS E VIESES COGNITIVOS

Os seres humanos não são agentes puramente racionais e suas decisões são frequentemente influenciadas por atalhos mentais e tendências a reações imediatistas. Embora estas estratégias mentais simplificadoras sejam úteis em determinadas situações, podem levar a erros sistemáticos e julgamentos inadequados.

As heurísticas são os atalhos mentais que agem de forma automática e intuitiva e permitem a tomada decisões de forma rápida, mas podem induzir a distorção do julgamento e levar a decisões equivocadas. Elas se baseiam em experiências passadas, crenças e valores intrínsecos do tomador da decisão. Segundo Kahneman (2012), as principais heurísticas incluem:

- Heurística da Representatividade: tendência a julgar a probabilidade de um evento com base em quão representativo ele é em uma categoria ou estereótipo;

- Heurística da Disponibilidade: tendência a julgar a probabilidade de um evento com base na facilidade com que exemplos relevantes vêm à mente; e

- Heurística do Afeto: tendência a tomar decisões com base em reações emocionais imediatas, em vez de uma análise mais detalhada.

Os vieses cognitivos são erros sistemáticos no processamento de informações por meio conceitos pré-concebidos ou ilusionais, afetando o julgamento e a tomada de decisão. Alguns dos principais vieses cognitivos incluem:

- Viés de Confirmação: tendência a buscar e interpretar informações de maneira a confirmar crenças e hipóteses pré-existentes;

- Viés do Status Quo: tendência a preferir manter o estado atual das coisas, evitando mudanças;

- Viés da Ancoragem: tendência a dar um peso desproporcional a uma informação ou valor inicial durante a tomada de decisão;

- Viés da Retrospectiva: tendência a superestimar a capacidade de prever um evento após ele ter ocorrido; e

- Viés da Aversão à Perda: tendência a dar mais peso a perdas potenciais do que a ganhos potenciais.

Por meio do reconhecimento da existência das heurísticas e vieses cognitivos como fenômenos psicológicos inerentes a todos os seres humanos e que afetam profundamente a tomada de decisão, podem ser desenvolvidas estratégias de preparação sobre os decisores, adoção de processos decisórios estruturados e elaboração de ferramentas de apoio à decisão que filtrem tais induções e diversifiquem as perspectivas de julgamento, contribuindo para fins de mitigar os seus efeitos negativos e promover decisões racionais e fundamentadas.

2.3 TEORIAS DA DECISÃO

Considerada como modelo teórico fundamental para a compreensão dos processos decisórios, especialmente em situações de incerteza, a Teoria da Utilidade Esperada foi originalmente introduzida por Bernoulli na busca atribuir uma função de matemática probabilística que compara o risco e a recompensa de cada escolha.

O desenvolvimento dessa teoria foi proposto por Von Neumann e Morgenstern (1953) partindo da premissa de que as pessoas tomam decisões racionais, buscando maximizar sua utilidade esperada por meio de atribuição de valores aos possíveis resultados de uma decisão, ponderados pelas respectivas probabilidades. Assim, a alternativa escolhida seria aquela com a maior utilidade esperada.

Levin (2006) destaca que esta teoria considera o conhecimento pleno dos riscos envolvidos e os resultados possíveis, limitando o campo das possibilidades. Tal condição, embora aplicável teoricamente, não abrange a incerteza inerente ao mundo real, em especial no ambiente de múltiplas decisões complexas.

Em que pese tais considerações, a Teoria da Utilidade Esperada continua sendo um modelo base útil para entender a tomada de decisão. Schoemaker (1982)

resume a importância dessa teoria, apesar de suas limitações, ao considerar que o modelo proposto produziu percepções mais profundas e questões mais refinadas, tanto descritiva quanto normativamente, a respeito de decisões sob risco, e revelou que as pessoas percebem e resolvem problemas de forma diferente.

Desafiando a noção de que os indivíduos tomam decisões de forma puramente racional da Teoria da Utilidade Esperada, Daniel Kahneman e Amos Tversky desenvolveram a Teoria Prospectiva, que busca explicar fenômenos, principalmente em condições de risco e incerteza, como a aversão a perdas, a preferência por opções seguras e a tendência a dar mais peso a informações recentes, ampliando a compreensão dos processos decisórios por meio do comportamento real das pessoas, levando em conta fatores psicológicos e cognitivos.

A Teoria Prospectiva se baseia em três principais efeitos que influenciam o processo de tomada de decisão:

a) Efeito Certeza: as pessoas tendem a dar mais peso a resultados certos do que a resultados prováveis, mesmo que estes tenham maior valor esperado. Explica que as pessoas tendem a preferir opções que garantem um resultado certo, mesmo que esse resultado seja menor, do que opções com maior potencial de ganho, mas com probabilidade inferior de ocorrência.

b) Efeito Reflexão: explica a tendência das pessoas de serem avessas ao risco quando se trata de ganhos, mas propensas ao risco quando se trata de perdas. Em outras palavras, teoriza que as pessoas tendem a dar mais peso psicológico a uma perda do que a um ganho de mesmo valor. Exemplificando, a sensação psicológica de se perder certa quantidade de dinheiro é geralmente maior do que a satisfação de ganhar a mesma quantidade.

c) Efeito Isolamento: refere-se à tendência das pessoas de focarem apenas em parte do problema ou da situação, deixando de considerar a totalidade das informações disponíveis. Isso faz com que a decisão pareça mais simples do que realmente é, levando a uma análise incompleta e potencialmente enviesada. As pessoas tendem a ignorar componentes comuns entre as alternativas e focar apenas nos aspectos que as diferenciam, destacando a tendência das pessoas de simplificar a análise ao focar em aspectos específicos, negligenciando a complexidade e a importância de considerar todas as informações relevantes para uma decisão informada e equilibrada.

A Teoria Prospectiva de Kahneman e Tversky representou uma importante contribuição para a compreensão dos processos decisórios, ao reconhecer a influência de fatores psicológicos e cognitivos no comportamento humano. Essa abordagem rompeu com a visão tradicional da racionalidade econômica e ampliou novas perspectivas para o estudo da tomada de decisão em diversas outras áreas.

Também proposta por Kahneman em colaboração com Tversky, foi proposta a Teoria da Perspectiva, uma expansão da Teoria Prospectiva, reconhecendo que as pessoas não avaliam as escolhas de forma racional, estatística e objetivamente, mas sim de maneira subjetiva, com base em como percebem as mudanças em relação ao ponto de referência de perda ou ganho.

Esse conceito é conhecido como efeito de quadros, se referindo à influência na percepção e decisão das pessoas de acordo com a forma da apresentação da alternativa. Por exemplo, as pessoas podem tomar decisões de maneira diferente se uma opção for apresentada como uma perda em vez de um ganho, mesmo que a situação subjacente seja a mesma. Kahneman (2012) constatou que as pessoas tendem a ser mais sensíveis às perdas do que aos ganhos equivalentes, significando que indivíduos são propensos a assumir riscos maiores para evitar perdas do que para obter ganhos, o que influencia suas escolhas e preferências. Trata-se da constatação de um fenômeno de natureza psicológica conhecido como “assimetria da sensibilidade às mudanças”.

A teoria da perspectiva, desenvolvida por Daniel Kahneman e Amos Tversky, tem sido fundamental na compreensão do processo decisório humano. Essa teoria destaca como as pessoas avaliam e tomam decisões com base em ganhos e perdas, em vez de avaliar objetivamente as probabilidades.

Ao considerar uma metodologia que permita que o decisor adote ações racionais diante de situações de incerteza, sem a necessidade de probabilidades objetivas, mas sim com base em suas próprias crenças subjetivas sobre os eventos futuros, a Teoria da Utilidade Esperada Subjetiva pode ser uma ferramenta valiosa para os líderes militares na tomada de decisões estratégicas e táticas, permitindo uma abordagem racional e adaptativa diante da incerteza e de cenários complexos.

Nesta égide, a capacidade profissional desenvolvida pelo decisor para se adaptar, refletir, questionar pressupostos para lidar com cenários paradoxais e caóticos, além de suas próprias crenças e julgamentos para estimar as probabilidades de eventos futuros, como o sucesso ou fracasso de uma operação, traz a subjetividade

do Comandante ou decisor como uma ferramenta relevante e aplicável ao processo decisório no campo militar.

Ao considerar um ambiente dinâmico e com necessidade de atualização das probabilidades de ocorrência de eventos de forma sistemática à medida que novas evidências são obtidas, surgiu a necessidade de aplicação de conceitos matemáticos mais refinados para apoio com dados empíricos ao decisor.

Neste sentido, o Teorema de Bayes apresenta um novo conceito teórico norteador, descrevendo a probabilidade de ocorrência de um evento com base em um conhecimento prévio relacionado a esse evento, desdobrando-se na Teoria da Decisão Bayesiana. Em essência, o Teorema de Bayes permite atualizar as probabilidades iniciais de um evento, chamadas de probabilidades a priori, à luz de novas evidências, resultando em probabilidades a posteriori. Isso significa que o Teorema de Bayes fornece um método sistemático para revisar e ajustar probabilidades e subjetividades sobre a ocorrência de um evento com base em novas informações. É amplamente utilizado em diversas áreas, como inferência estatística, *machine learning*, e análise de dados, constituindo-se uma ferramenta poderosa para lidar com incertezas e atualizar conhecimentos.

Em uma modelagem matemática, a fórmula do Teorema de Bayes pode se definida por:

$$P(A|B) = (P(B|A) * P(A)) / P(B)$$

Onde:

- $P(A|B)$ é a probabilidade de A dado que B ocorreu (probabilidade a posteriori)
- $P(B|A)$ é a probabilidade de B dado que A ocorreu
- $P(A)$ é a probabilidade a priori de A
- $P(B)$ é a probabilidade total de B

A aplicação desta fórmula permite calcular a probabilidade de um evento A ocorrer, dado que outro evento B já ocorreu, levando em conta o conhecimento prévio sobre as probabilidades de A e B.

Além da consideração das probabilidades subjetivas, a aplicação da Teoria da Decisão Bayesiana permite a atualização sistemática de novas evidências, ocasionando a minimização do risco ou da probabilidade de erro e a maximização do resultado esperado, além de fornecer um arcabouço formal e validado para a tomada de decisão em cenários de incerteza.

De acordo com Gross (2010), durante a Segunda Guerra Mundial, alguns problemas dos aliados, de ordem tática e estratégica, eram muito complexos para serem abordados pelas teorias apresentadas. Nesse contexto, surgiu a ideia de trabalhar com grupos multidisciplinares, envolvendo cientistas de várias áreas de conhecimento que, atuando com visão sistêmica e metodologia científica, tratavam questões práticas da guerra, como por exemplo a melhor forma de utilizar os radares, como organizar as baterias antiaéreas e como melhor dimensionar as frotas.

Nesse contexto de complexidade nas decisões que possuem múltiplas variáveis e envolvam critérios qualitativos, surgiu o conceito de decisão multicritério, a qual fornece ferramentas, técnicas e procedimentos racionais que auxiliam o processo decisório, permitindo uma abordagem mais abrangente, integrada e ponderada.

Uma importante contribuição do método multicritério no apoio à decisão reside na possibilidade de integração de divergências e diversidades, considerando a utilização de múltiplos decisores com diferentes juízos de valores e, por vezes, pontos de vista conflitantes, podendo gerar soluções disruptivas.

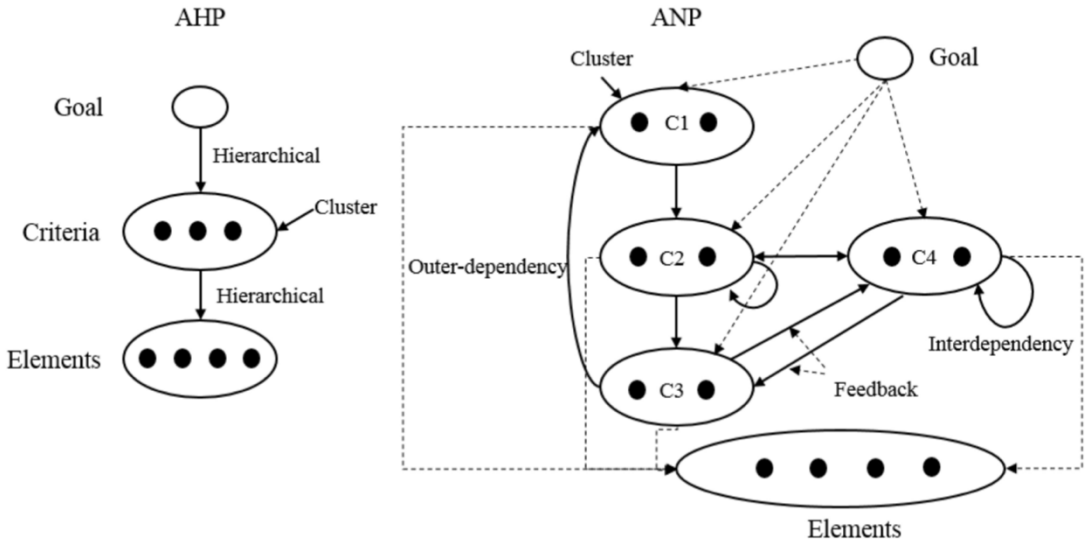
Um dos principais teóricos sobre a decisão multicritério é Thomas L. Saaty. Ele é conhecido por desenvolver o Processo da Análise Hierárquica (AHP, do inglês *Analytic Hierarchy Process*), uma metodologia que propõe a decomposição do problema de decisão em uma hierarquia de critérios e subcritérios, onde os critérios são organizados em uma estrutura de árvore. Os tomadores de decisão então avaliam as alternativas em relação a cada critério usando escalas de comparação de preferência, geralmente na forma de matrizes de julgamento.

Um aspecto a ser considerado na estruturação segundo o método AHP consiste na presença da subjetividade no estabelecimento dos critérios e na definição dos pesos na hierarquização. Por mais que os cálculos possam ser otimizados e automatizados, este modelo ainda requer elementos da percepção subjetiva baseados no conhecimento de especialistas e da experiência operacional que devem estar presentes no processo decisório.

Como uma evolução do AHP, Saaty (1990) também desenvolveu o Processo de Análise em Rede (ANP, do inglês *Analytic Network Process*), segundo o qual é possível tratar de situações em que os elementos inferiores impactam os de nível superior do modelo hierárquico ou em que os elementos do mesmo nível não são independentes. Essa abordagem permite a fusão de relacionamentos que podem ser

organizados em *clusters*, criação de relações de dependência e *feedbacks* entre os critérios e alternativas, de uma forma a contabilizar as relações de interdependência entre diferentes níveis de decisão em formato de rede. A figura 2 representa estas teorias em sua forma estrutural simples.

Figura 2 – Diferenças entre estruturas AHP (a) e ANP (b)



Fonte: Hwang, Han e Chang, 2020

Segundo Yüksel e Dağdeviren (2007), AHP e ANP são metodologias estatísticas para medir variáveis intangíveis por meio de comparações par-a-par com atribuições de prevalência de um elemento sobre outro com respeito a uma propriedade que eles compartilham, sendo o método ANP uma generalização do AHP que considera interações complexas entre níveis de decisão e atributos.

2.4 TEORIAS DE DECISÃO APLICADAS COM FERRAMENTAS DE APOIO À DECISÃO

O conceito de racionalidade limitada apresentado por Simon expôs a incapacidade dos indivíduos de considerar todas as alternativas disponíveis devido a restrições cognitivas e de tempo.

Os sistemas mentais propostos por Kahneman demonstraram que o raciocínio humano pode ser rápido e instintivo ou lento e ponderado, com limitações intrínsecas e sujeitos à heurísticas e vieses cognitivos.

Ao apresentar as principais teorias da decisão, tais como a Teoria da Utilidade Esperada, a Teoria Prospectiva, a Teoria da Perspectiva, a Teoria da Decisão Bayesiana, além dos métodos de decisão multicritério AHP e ANP, foi possível identificar a presença constante da subjetividade no processo decisório e o desafio de quantificá-la objetivamente por modelos estatísticos como forma de se obter a melhor solução possível.

Neste sentido, o emprego de ferramentas tecnológicas de apoio à decisão permite superar as limitações mentais inerentes aos humanos e otimizar os resultados de forma racional, devendo integrar a complexidade da subjetividade humana com a objetividade dos dados, propondo soluções mais rápidas e ponderadas. Ao mitigar heurísticas e vieses por meio de modelagem objetiva e estatística, elas resultam em propostas decisórias equilibradas, eficazes e confiáveis.

No próximo capítulo serão apresentadas as novas ferramentas tecnológicas que apresentam potencial disruptivo de capacidade processamento, mas que devem ser estruturadas em requisitos de confiabilidade específicos para segurança em sua utilização, em especial ao tratar de processos que envolvam apoio às decisões militares.

3 PERSPECTIVAS TECNOLÓGICAS

A tecnologia tem sido uma constante impulsionadora do progresso humano, moldando e redefinindo a forma como vivemos, trabalhamos e nos comunicamos. Desde o domínio do fogo até a era digital, cada inovação trouxe consigo transformações profundas e impactantes.

Neste capítulo, será apresentado um breve histórico do desenvolvimento tecnológico, com ênfase no emprego das novas ferramentas em sistemas de apoio à decisão, destacando as potencialidades e desafios desse novo horizonte de possibilidades.

3.1 TECNOLOGIA TRANSFORMADORA DA SOCIEDADE

Ao longo da história da civilização ocorreram diversos eventos que mudaram a forma de interação humana com a natureza e com a própria sociedade. O domínio do fogo, a invenção da roda, o desenvolvimento de ferramentas rudimentares de pedra, além das técnicas de irrigação, de construção de abrigos para proteção contra predadores e inimigos são alguns exemplos de avanços tecnológicos que foram transformadores para a humanidade.

Desde épocas muito anteriores aos modernos computadores conhecidos atualmente, existem registros da utilização de instrumentos e ferramentas para fins de contagem, armazenagem e análise de dados. Em 1960, foi descoberto em Uganda um artefato denominado “Osso de Ishango”[1], com data estimada de 18.000 anos A.C., sendo considerado uma das primeiras evidências de armazenamento de dados pré-históricos. Considera-se que bastões ou ossos eram utilizados para acompanhar as atividades de comerciais, por meio dos quais os comparavam para realizar cálculos e permitindo-lhes fazer previsões de estoque de alimentos.

Parafraseando Benjamin Franklin (1706-1790), Amarante (2009) descreve que a adaptação da espécie humana ao planeta e as modificações do *habitat* foram

[1] Trata-se de artefato arqueológico composto de um osso de fíbulas de babuíno contendo uma série de entalhes que se acredita ter sido utilizado para fins matemáticos, astronômicos ou uma ferramenta para registros e cálculos simples.

amparadas e viabilizadas por meio da tecnologia, considerando como característica fundamental do *Homo Sapiens* como um “fazedor de ferramentas”.

Com o advento da Revolução Industrial, houve uma rápida expansão da tecnologia em diversas áreas. No campo militar verificou-se o desenvolvimento de armas mais avançadas, tais como rifles, metralhadoras e canhões, além de surgimento de outros equipamentos de uso comum, como telégrafos e locomotivas, que ampliaram as capacidades de comunicação, logística e mobilização militar.

No século XX, mormente durante as duas grandes guerras mundiais, a tecnologia desempenhou um papel determinante no resultado dos conflitos, com inovações como o rádio, o sistema de detecção radar, a criptografia nas comunicações e o crescimento da aplicação de sistemas computacionais para a comunicação, inteligência e estratégia militar. Em verdade grande parte das tecnologias desenvolvidas foram verdadeiros *spin-offs*[2] do advento da tecnologia eletrônica de estado sólido, caracterizada pelo desenvolvimento do transistor.

Segundo Kurzweil (2005), o ritmo de mudança na tecnologia criada pelo homem está acelerando e suas capacidades se expandem em ritmo exponencial. Computadores já realizam precisos diagnósticos em eletrocardiogramas e em complexas imagens médicas, arbitram decisões de crédito financeiro, “pilotam” aeronaves em sistemas não-tripulados (SNT), podem executar decisões táticas de armas automáticas em sistemas de autodefesa e de armas letais autônomas (do inglês *Lethal Autonomous Weapon Systems* – LAWS), avançando em tarefas e níveis de responsabilidade crítica que, por muitas vezes, costumavam precisar de aptidões humanas e, ainda, com habilidades para resolver problemas da inteligência cognitiva, emocional e moral do próprio cérebro humano.

Gordon E. Moore (1965), cofundador da Intel, conceituou o que vem sendo conhecido como a Lei de Moore. Em sua abordagem, o número de transistores num circuito integrado tenderia a dobrar a cada 2 anos e seu custo tenderia a reduzir pela metade no mesmo período. Além da constatação desta tendência, por meio dos inegáveis avanços tecnológicos experimentados nas últimas décadas, este conceito alerta para a questão de tempo de projeto para o desenvolvimento e aplicação de

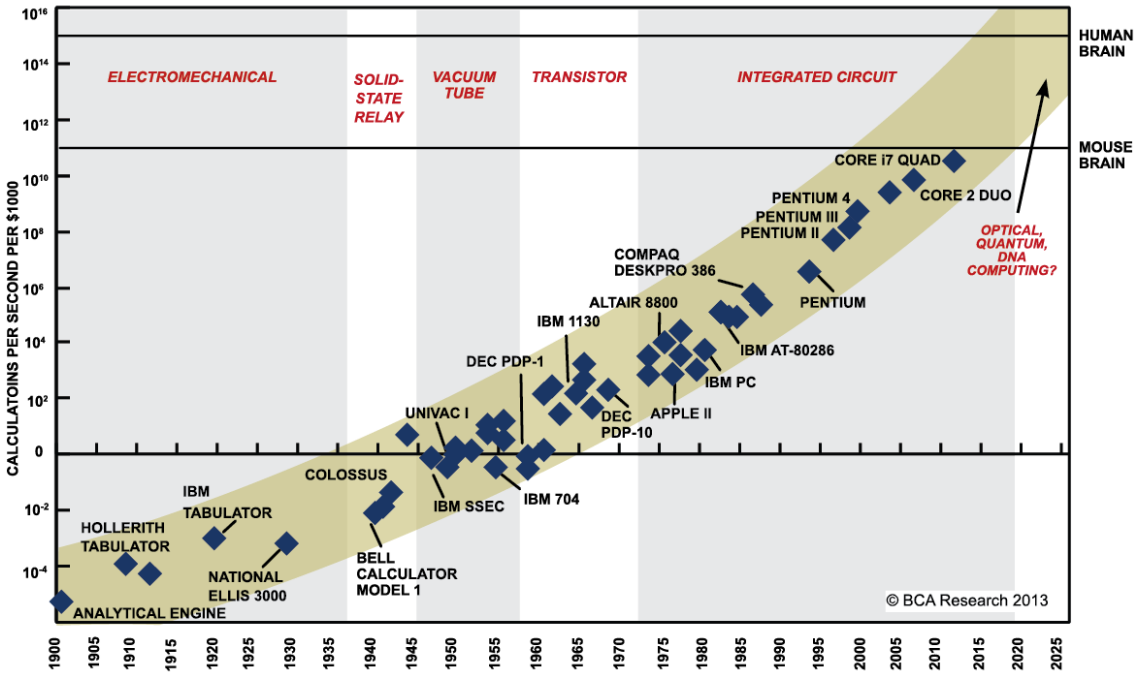
---

[2] Refere-se ao termo utilizado para descrever o desdobramento de um novo empreendimento a partir de outro, podendo ser utilizadas em diferentes contextos, como nos negócios, entretenimento, tecnologia e indústria.

novas tecnologias, indicando a janela de oportunidade e de obsolescência tecnológica para, em épocas atuais, um ciclo de 4 anos. Ademais, a Lei de Moore direciona para o conceito da “singularidade” proposto por Kurzweil (2005), segundo o qual o ritmo da mudança tecnológica será tão rápido e com impacto de tal profundidade, que ocorrerão mudanças irreversíveis em diversos setores da sociedade, transformando desde modelos de negócios até o ciclo da vida humana, incluindo a definição da morte.

A figura 3 apresenta a evolução ao longo dos séculos XX e XI da capacidade de processamento de dados em um custo fixo, citando o desenvolvimento da Máquina de Tabulação de Hollerith[3] na era dos dispositivos eletromecânicos, o surgimento do transistor e, posteriormente, do circuito integrado, permitindo o desenvolvimento e produção de diversos equipamentos em grande escala, com diminuição significativa do consumo de energia, maior robustez física e expansão da capacidade de armazenamento de dados, com conformidade à Lei de Moore.

Figura 3: Evolução do processamento de dados



Fonte: https://www.extremetech.com/extreme/210872-extremetech-explains-what-is-moores-law. Acesso em: 20 abr. 2024

[3] Dispositivo inventado por Herman Hollerith em 1889, considerado um precursor dos computadores atuais. Foi projetado para ajudar a automatizar a compilação e análise de grandes volumes de dados, utilizando cartões perfurados e processo de leitura eletromecânica.

A exponencialidade apresentada pela Lei de Moore, comprovada pela realidade do desenvolvimento tecnológico, permitiu a ampliação do conhecimento em diversos outros domínios, como a criação de ambientes de realidade aumentada, de sistemas satelitais de vigilância, de monitoramento e georreferência em escala global, armas biológicas, artefatos nucleares de emprego tático, sistemas bélicos hipersônicos, veículos remotamente tripulados ou autônomos, sistemas de defesa cibernética e tecnologias de IA. Essas tecnologias estão sendo cada vez mais integradas à sociedade e se tornando determinantes às operações militares em termos de eficácia, precisão e redução do risco para as tropas. Além disso, apresentam novas possibilidades de melhoria do processo decisório e a tomada de decisões, alterando a natureza, a condução e os resultados dos conflitos militares.

3.2 NOVAS TECNOLOGIAS

A desconfiança, a resistência às mudanças, a falta de conhecimento, os riscos, as incertezas e a falta de confiabilidade são algumas das principais barreiras enfrentadas para a implementação de novas ferramentas tecnológicas, demandando maior clarificação e argumentação fundamentada para os níveis decisores e formuladores de políticas e estratégias, por meio da apresentação das potencialidades e vantagens competitivas que podem ser empregadas nos mais variados cenários.

A implementação de tecnologias inovadoras e disruptivas como *Big Data*, IA, *machine learning* (ML) e *deep learning* (DL) se depara com desafios dessa natureza, na medida em que podem propor novos arranjos em estruturas já consolidadas e possibilidades ainda não exploradas, além de novos riscos e falhas de confiabilidade ainda não vivenciadas, seja no campo administrativo, técnico ou operacional.

3.2.1 *Big Data*

A Biblioteca de Alexandria já foi considerada a maior coleção de dados do mundo antigo, abrigando cerca de meio milhão de rolos de papel que abrangiam um pouco de tudo o que era conhecido à época. Tratava-se nada menos que o repositório cultural da história da humanidade que, talvez acidentalmente, em 48 d.C., acredita-se que tenha sido destruída pelos invasores romanos. Não havia cópias, registros

físicos em outros lugares, backups de segurança ou os atuais armazenamentos em memórias digitais ou arquivos compartilhados em nuvem para fins de recuperação dos dados. Consequentemente, muitos registros e conhecimentos da humanidade foram perdidos para sempre.

Com as devidas ressalvas na comparação, propor uma analogia anacrônica entre a Biblioteca de Alexandria e o conjunto massivo de dados de um sistema de apoio à decisão permite compreender a dimensão e a relevância do armazenamento seguro das informações. Assim como a Biblioteca de Alexandria foi um repositório crucial de conhecimento no mundo antigo, o *Big Data* representa, de forma muito simplificada, um ambiente de armazenagem de um massivo volume de informações organizadas. A perda de dados pode ter um impacto devastador e irreparável para uma organização, destacando a relevância de sistemas confiáveis de armazenamento e gerenciamento de informações.

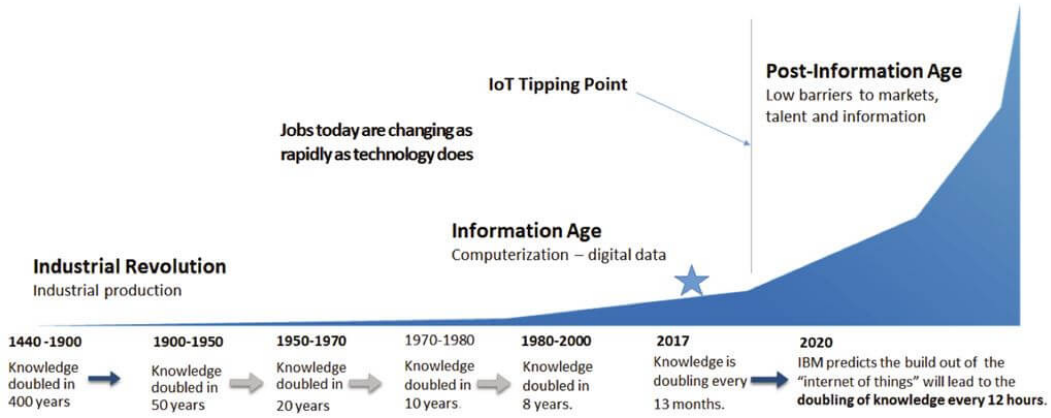
No livro "*Critical Path*", Fuller (1982) apresentou o conceito da curva de duplicação do conhecimento, destacando o impulsionamento para um crescimento exponencial devido aos avanços tecnológicos e de comunicação global, apresentando aderência à Lei de Moore. Em suas observações, Fuller constatou que até 1900 o conhecimento humano dobrava aproximadamente a cada século e que após a Segunda Guerra Mundial a taxa de duplicação começou a acelerar, conforme representado na figura 4. Schilling (2013) destaca que, de acordo com a IBM, a construção da IoT[4] (*Internet of Things*) levará à duplicação do conhecimento a cada 12 horas.

Dos diversos fatores que contribuíram para esta aceleração do conhecimento, destacaram-se o desenvolvimento dos computadores, da internet e das redes sociais, tecnologias que potencializaram a criação, o armazenamento e o compartilhamento de ideias em escala global. Suas implicações provocaram profundas transformações no sistema educacional, no trabalho e na economia, exigindo cada vez mais a adaptação das pessoas e das empresas às inovações tecnológicas, trazendo novas oportunidades e desafios associados.

---

[4] Refere-se ao modelo de interconexão de dispositivos por meio da internet para fins de compartilhar dados uns com os outros.

Figura 4 – Curva da duplicação do conhecimento



Fonte: https://www.psicologiafacile.com/lintelligenza-artificiale-e-il-fallimento-cognitivo-dellessere-umano/. Acesso em: 20 abr. 2024

Por volta de 2005 entramos na era da Web 2.0, momento em que diversas empresas começaram a perceber a extensão do volume de dados gerados e utilizados pelos usuários e outros serviços *online*. Considerando, ainda, que se tratava de conjuntos de dados de todos os tipos, as tecnologias de armazenamento e bancos de dados tradicionais disponíveis à época não eram capazes de processá-los e analisá-los, sendo necessárias novas estruturas para comportar essas novas demandas. Neste sentido, grandes empresas como a Google e Yahoo! passaram a desenvolver novos modelos de arquitetura de armazenamento, organização, processamento e disponibilização de dados, estruturados ou não, e que deveriam ser capazes de atualização dinâmica, nascendo o conceito do *Big Data*.

A principal entrega do *Big Data* está em sua capacidade de fornecer novas ideias e possibilidades por meio de análise de registros empíricos em larga escala, permitindo identificar tendências, realizar predições baseadas em dados, desenvolver novas estratégias de negócios mais precisas e tomar decisões baseadas no maior número de informações disponíveis.

Das capacidades advindas da utilização do *Big Data* deriva o conceito estratégico denominado *Data Driven*. Segundo a empresa de consultoria TOTVS, não se trata de um método, mas sim uma cultura de gestão corporativa que envolve basear as decisões da empresa em dados mensuráveis. Entre as diversas vantagens deste conceito, cita-se a otimização de recursos e processos, redução de custos, planejamento adaptativo ágil, identificação de tendências e previsão de cenários

futuros, recursos que permitem vantagens competitivas para o mundo dos negócios e com diversas aplicações no ambiente militar.

No entanto, em que pese as enormes possibilidades, a qualidade dos dados, a robustez do sistema, a garantia da privacidade e segurança dos dados, a utilização de filtros complexos para dados espúrios ou incorretos, além da criação de estruturas éticas e regulatórias para o uso responsável das informações, ou seja, a sua confiabilidade em amplo espectro, representa um novo desafio para os projetistas e usuários dos sistemas. Para estruturas com culturas hierarquizadas, soma-se ainda o desafio da mudança da cultura organizacional pela perspectiva relativa da desumanização e possível redução do poder de decisão.

Com os devidos conhecimentos e procedimentos técnicos para fins de superar os desafios da aplicação do *Big Data* descortinam-se novas possibilidades na tomada de decisões no campo militar, sejam estratégicas, operacionais ou táticas. A possibilidade da identificação de tendências, oportunidades e ameaças em tempo real, permitirão operações mais seguras, precisas e adaptáveis às condições dinâmicas do campo de batalha.

3.2.2 Inteligência Artificial (IA)

Estima-se que, em meados dos anos 300 a.C., em seus estudos e reflexões filosóficas sobre a forma de como se processa o raciocínio humano, Aristóteles propôs um modelo básico de formatação do pensamento lógico composto por um sistema com dois argumentos fundamentais, denominados premissas, que por derivação sob regras definidas permitia-se chegar a uma conclusão, processo conhecido como lógica silogística, a qual serviu por séculos como pedra fundamental para o desenvolvimento do pensamento estruturado da civilização ocidental.

Passados mais de 2 mil anos, Warren McCulloch e Walter Pitts, em 1943, publicaram um artigo intitulado de “*A Logical Calculus of the Ideas Immanent in Nervous Activity*”, o qual, segundo Piccinini (2004), apresenta um modelo matemático estruturado na lógica do processamento de informações pelos neurônios e pelo sistema nervoso humano, uma abordagem que estabeleceu a base teórica para a construção das redes neurais artificiais e a apresentação de seu imenso poder

computacional, aspectos fundamentais para o desenvolvimento da computação e da ciência cognitiva.

Em 1950, considerando as possibilidades e desafios advindos das tecnologias que surgiam, o matemático inglês Alan Turing, por meio do artigo intitulado "*Computing Machinery and Intelligence*", formulou o célere questionamento: "As máquinas podem pensar?". Esse trabalho é considerado pioneiro na exploração sobre as possibilidades fundamentais das máquinas em aprender e aplicar a sua própria "inteligência" na resolução de problemas.

Com o objetivo de obter uma resposta prática ao questionamento, Turing desenvolveu o chamado "Jogo da Imitação", também conhecido como Teste de Turing. O objetivo era determinar se uma máquina pode apresentar um comportamento reativo e inteligente de forma compatível com a de um ser humano. Caso a máquina obtenha êxito, ou seja, apresentar a habilidade de imitar o comportamento humano de forma convincente segundo os parâmetros do teste, ela é considerada "inteligente" e aprovada no teste. Mesmo sendo uma verificação de IA original, uma vez que se baseia mais na capacidade de simular comportamentos humanos, a metodologia do Teste de Turing não avalia aspectos relacionados à compreensão ou consciência verdadeiras.

A ideia de uma máquina com a capacidade de executar tarefas e replicar inteligência humana despertou a atenção e gerou reflexões em diversas áreas da sociedade. No mesmo ano do artigo de Turing, Isaac Asimov publica "Eu, Robô", uma coleção de contos de ficção científica que introduziu as Três Leis da Robótica, abordando dilemas éticos e conflitos morais entre robôs dotados de inteligência e interação com os humanos. Em outra abordagem, em 1968, Stanley Kubrick lança o filme "2001: Uma Odisseia no Espaço", apresentando uma perspectiva filosófica sobre a evolução humana, conceitos de máquinas gerenciando rotinas complexas e auxiliando o processo de tomada de decisão, além de projetar o futuro da exploração espacial. Tais obras, distintas em mídia e abordagem, contribuíram para moldar a percepção pública de temas como a tecnologia, o futuro da humanidade e as questões éticas que acompanham esses avanços.

Em 1956, durante a Conferência de Dartmouth, John McCarthy utilizou pela primeira vez a expressão "*Artificial Intelligence*", sendo considerado pela comunidade acadêmica como marco-zero para o termo. O evento reuniu diversos pesquisadores renomados e interessados em redes neurais e inteligência, sendo estabelecida a IA

como um novo campo de estudo. Em sua proposição, IA seria a ciência e engenharia de fabricação de máquinas inteligentes, especialmente programas de computador inteligentes (McCarthy, 2007).

Do conceito proposto por McCarthy e de diversos outros pesquisadores, todos se alinham ao entendimento de que a IA está relacionada com uma tecnologia que habilita computadores e máquinas a capacidade de simulação da inteligência humana, possuindo a capacidade de resolução de problemas sem intervenção. Em síntese, segundo Luger (2013), a IA pode ser definida como o ramo da ciência da computação que se ocupa da automação do comportamento inteligente.

Novas aplicações para IA ainda estão sendo descobertas, disponibilizadas à sociedade e aprimoradas em escala acelerada. As correlações interdisciplinares de sua aplicações permitiram o desenvolvimento de outras tecnologias, tais como:

a) assistentes virtuais – ferramentas como a Siri, Alexa e outros assistentes com reconhecimento de voz, executadas em linguagem natural e em vários idiomas, permitem a organização e realização de tarefas, além de fornecer informações baseadas em dados pré-configurados ou por meio de algoritmos de busca autônomos que podem aprender e melhorar com o tempo;

b) reconhecimento biométrico – desenvolvimento de técnicas baseadas em processamento de grande volume de dados baseados em impressões digitais, reconhecimento facial e outros parâmetros biométricos individuais que estão sendo aplicados em sistemas de segurança e autenticação;

c) geração de imagens e cenários – emprego de modelagens matemáticas para a criação imagens em alta resolução que podem ser incorporados em ambientes dinâmicos, podendo ser empregados em áreas de marketing, design gráfico e de simulação;

d) veículos e dispositivos autônomos – o emprego integrado de sensores óticos, infravermelhos, radares e técnicas de georreferenciamento com sistemas computacionais, permitiu o desenvolvimento de meios com capacidade de identificação do ambiente, dotando-os da capacidade de navegação sem a necessidade de intervenção humana. Essa tecnologia está revolucionando as possibilidades de aplicação na mobilidade urbana e em sistemas de armamentos; e

e) medicina de precisão – a capacidade de correlação de dados em larga escala associada ao potencial de simulações estatísticas da IA está permitindo avanços no diagnóstico antecipado e preciso de doenças, no desenvolvimento de

novos medicamentos e de tratamentos personalizados. Em aplicações militares, dispositivos que monitoram em tempo real das condições fisiológicas de elementos da tropa permitirão novas aplicações e perspectivas para a medicina de combate, além de contribuir para a ampliação da consciência situacional no campo de batalha.

Considerando aspectos semânticos dos conceitos e das terminologias, torna-se fundamental explicar a diferenciação entre o que são sistemas automáticos e sistemas autônomos. Embora sejam conceitos relacionados pela não intervenção humana na fase execução de uma operação, possuem significados diferentes no que tange à base de dados utilizada. Em síntese, sistemas automáticos são projetados para seguir regras fixas, programações predefinas e atividades repetitivas, sem possuir capacidade de adaptação a mudanças que não estiverem sido previamente definidas, sendo eficazes em ambientes estáveis e previsíveis. Por sua vez, os sistemas denominados autônomos possuem a capacidade de se adaptar ao seu ambiente por meio de coleta de dados de forma dinâmica, da análise interpretativa, do reconhecimento de padrões, da interação com outros sistemas e da tomada de decisões baseadas no processamento desse novo conjunto dados. Eles podem se adaptar e combinar novas situações, aprimorando o seu desempenho por meio de aprendizado por *feedback* comparativo de resultados anteriores.

Paradoxalmente, além das novas perspectivas de emprego da IA para a solução e otimização de problemas que não eram possíveis até alguns anos atrás, a sua implementação se desdobra para além dos desafios técnicos e de custos, trazendo consigo um novo conjunto de temáticas controversas e impactantes, tais como erros decorrentes de vieses algorítmicos, a falta de transparência do processamento, a possibilidade de ocasionar problemas econômicos e sociais pelo desemprego de trabalhadores humanos em diversas áreas, além de questões morais, éticas e jurídicas, demandando novos desafios para sociedade.

Em contrapartida, a visão de Li et al. (2023) direciona para uma perspectiva otimista, pois argumenta que o rápido desenvolvimento da IA continua a proporcionar benefícios econômicos e sociais vantajosos à sociedade. Com a sua aplicação generalizada em áreas como transportes, finanças, medicina, segurança e entretenimento, há uma consciência crescente da sociedade de que estes sistemas sejam confiáveis, mas ressalta que a quebra da confiança das partes interessadas pode levar a graves consequências sociais. Tais violações podem variar desde o tratamento tendencioso ou inexecutáveis por sistemas automatizados em decisões

simples até a tomada de decisões autônomas complexas que podem ocasionar a perda de vidas humanas.

3.2.3 *Machine Learning* (ML) e *Deep Learning* (DP)

Segundo Chollet (2018) o conceito do aprendizado de máquina é bastante antigo, tendo surgido com o questionamento sobre a capacidade de um computador executar ações além do que foi programado e aprender de forma autônoma em como executar uma nova tarefa. Dessa forma não haveria mais a necessidade de programadores para o desenvolvimento de softwares ou o processamento de dados de forma manual.

Em 1952, Arthur Samuel, desenvolveu um programa para um computador da IBM jogar damas. A característica marcante deste programa era a capacidade de melhorar o desempenho à medida que jogava e registrava novos parâmetros, ou seja, adquiria mais “experiência” ou “aprendia”.

No entanto, somente em 1959 que Samuel utilizou o termo ML ou aprendizado de máquina pela primeira vez. Em sua abordagem, ML é definido como um campo de estudo que dá aos computadores a habilidade de aprender sem terem sido programados para tal. Com uma definição mais abrangente e atual, Srinivasaraghavan (2020) define ML como uma área da ciência da computação que envolve ensinar computadores a aprender por meio da experiência, transformando dados em informações por meio de algoritmos de aprendizado que coletam novas informações de forma autônoma e melhoram seu desempenho de forma contínua e adaptativa.

O processo de desenvolvimento de uma rotina computacional por um programador humano é um trabalho exaustivo, complexo, demorado, sujeito a falhas, caro e, por vezes, com limitações para atualização. Neste cenário, o aprendizado de máquina apresenta-se como uma tecnologia disruptiva, pois permite que os computadores possam “treinar” e “aprender” automaticamente a partir de experiências ou dados que não foram inseridos em sua programação original por meio de modelos matemáticos e estatísticos.

Shalev-Shwartz e Ben-David (2014) abordam a aprendizagem de máquina como um domínio amplo, apresentando uma taxonomia para definir os diversos tipos de aprendizagem, sendo eles:

- Supervisionado *versus* Não Supervisionado: na aprendizagem supervisionada são apresentados exemplos bem definidos de entradas rotuladas e as saídas são conhecidas, ensinando o algoritmo a comparar seu resultados para fins de identificar erros e aprimorar o modelo. Nesta abordagem, a aprendizagem ocorre por um processo de “usar a experiência para ganhar conhecimento”. Na aprendizagem não supervisionada, os dados são apresentados de forma bruta, não rotulados, de forma que o algoritmo de aprendizagem busque variáveis em comum entre eles por meio de busca de padrões ocultos, “aprendendo” a definir novos padrões. Existe, ainda, uma tipologia intermediária denominada aprendizado por reforço (*Reinforcement Learning*) que, relacionada aos princípios do behaviorismo, executa rotinas de interações entre estímulo e resposta, de forma a moldar o comportamento algorítmico por meio do reforço positivo ou negativo.

- Passivo *versus* Ativo: Em um ambiente passivo o algoritmo apenas recebe informações fornecidas pelo ambiente, sem influenciá-lo ou direcioná-lo. Já em um ambiente ativo, o algoritmo interage com o ambiente no momento do treinamento por meio de questionamentos, correlações de dados e experimentos estatísticos, potencializando o aprendizado quando os dados rotulados são escassos.

- Aprendizagem adversária: Abrange o conceito de que a aprendizagem também ocorre quando se utiliza um algoritmo “adversário” que efetua indução de comportamento errático ou aproveitando-se de falhas ou lacunas de dados, forçando com que o algoritmo “aprendiz” desenvolva novas correlações e padrões de filtros. Pode ser considerado um aprendizado por reforço “forçado” por um adversário, sendo empregado em sistemas de prevenção de fraudes.

- Aprendizagem *Online* (*Online Learning*) versus Aprendizagem em Lote (*Batch Learning*): A aprendizagem online é um modelo que utiliza uma base de dados com cenários dinâmicos que se atualizam de forma contínua e em tempo real, sendo utilizados em ambientes em que os dados mudam rapidamente, como *trading* financeiro ou operações militares. Na aprendizagem em lote, o aprendizado do algoritmo ocorre de forma análoga a uma atualização periódica, segundo a qual os novos dados são apresentados em momento específico e, geralmente, possuindo grande volume. Este modelo é aplicável em ambientes estáticos ou com pouca variação.

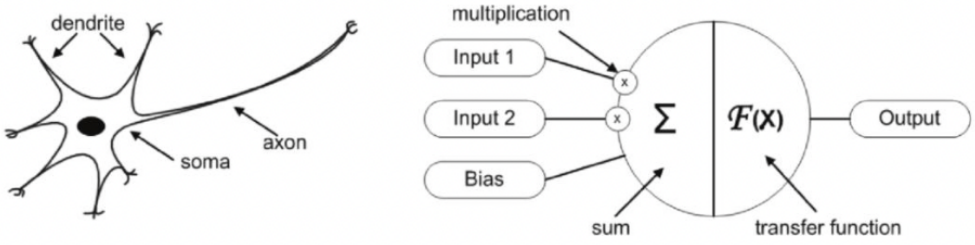
Entre as abordagens estruturais mais utilizadas de ML, tais como árvore de decisão, programação lógica indutiva, agrupamento e redes Bayesianas, destaca-se

o *Deep Learning*, um modelo de aprendizagem que tem se demonstrado mais adequado em tarefas que envolvem reconhecimento de padrões complexos, como reconhecimento facial, de fala, recomendações personalizadas e diagnósticos de saúde por imagens.

A estruturação lógica do *Deep Learning* é baseada na utilização de camadas de processamento e inspirado nas formas de conexões biológicas dos neurônios do cérebro humano. Para tal, os algoritmos são desenvolvidos e conectados em rede de lógica computacional, possuindo capacidade de interação entre si de forma análoga aos neurônios biológicos, estrutura conhecida como Rede Neural Artificial (RNA). Os níveis das estruturas interdependentes e correlacionadas são chamados de camadas de uma RNA, definindo o seu grau de profundidade.

Krenker et al. (2011) destaca as semelhanças lógicas entre um neurônio biológico e um “neurônio artificial” (elemento básico de rede neural artificial), conforme figura 5.

Figura 5: O neurônio biológico e o neurônio artificial



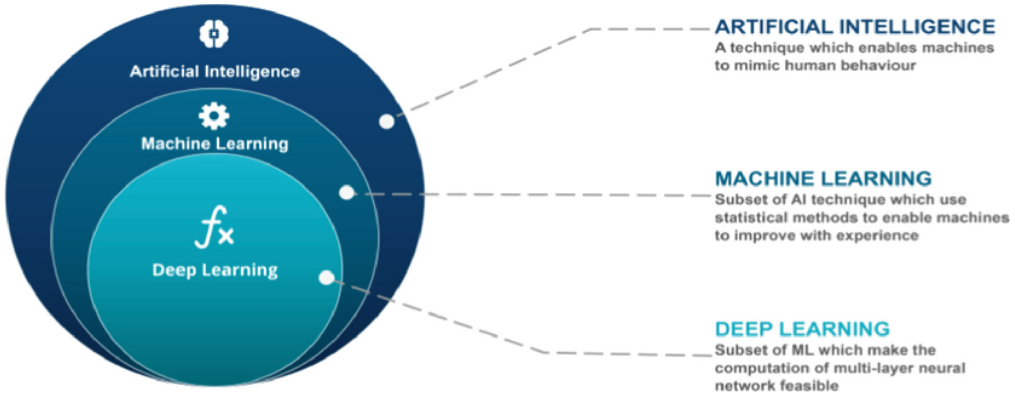
Fonte: Krenker et al., 2011

No neurônio biológico, a entrada de dados ocorre pelo dendrito, o processamento ocorre no corpo do neurônio e a transmissão ocorre via axônio. Em um neurônio artificial, as entradas são ponderadas individualmente, processadas por uma lógica computacional específica e adaptável, produzindo saídas emuladas por uma função de transferência.

Devido sua capacidade de analisar um grande volume de informações não previamente categorizadas ou hierarquizadas, o *Deep Learning* tem sido explorado para criar soluções inovadoras em tecnologia da informação (TI), *insights* de alternativas não triviais ou ocultas para o auxílio ao processo decisório e potencializar as inovações em diversas áreas.

Em resumo, a IA, o ML e o DL são conceitos relacionados, sendo a IA o campo geral que habilita as máquinas a replicar o comportamento humano, o ML como um subcampo da IA que se concentra os métodos do aprendizado a partir de dados, e o DL sendo uma técnica mais avançada de ML que utiliza redes neurais profundas, conforme demonstrado na figura 6.

Figura 6: Relação entre IA, ML e DL



Disponível em: https://www.edureka.co/blog/ai-vs-machine-learning-vs-deep-learning/. Acesso em: 18 jun. 2024

3.3 RISCOS E INCERTEZAS

Em 1968 era lançado o filme "2001: Uma Odisseia no Espaço", de Arthur C. Clarke, tendo como um dos protagonistas o supercomputador HAL 9000. Dotado de uma IA avançada, HAL controlava as principais funções de uma nave espacial e gerenciava os mecanismos de suporte à vida dos astronautas embarcados. Mesmo tendo sido construído com a maior tecnologia humana disponível e com o conceito de ser à prova de falhas, HAL começou a executar rotinas erráticas e exibir traços de comportamentos humanos, despertando a atenção da tripulação, que decidiu desligá-lo. O aprendizado de HAL direcionou para a conclusão de que ele era essencial para o cumprimento da missão e os astronautas se tornaram uma ameaça, vindo a decidir por eliminá-los.

Além da reflexão sobre a confiabilidade técnica e os limites do controle humano sobre suas criações tecnológicas, a trajetória de HAL levanta questões morais, éticas e filosóficas profundas sobre o comportamento das inteligências artificiais, sugerindo conflitos de interesse que podem representar um potencial de perigo catastrófico por violação funcional de regras algorítmicas de segurança.

Em situações complexas, de múltiplas variáveis e com evolução dinâmica, os resultados de estratégias, ações ou decisões podem não obedecer a uma linearidade pré-concebida, podendo se desdobrar em efeitos diversos da sua motivação inicial. Tais efeitos podem, inclusive, potencializar ou minimizar a própria ação inicial, travando uma relação biunívoca de ciclos indefinidos e que se retroalimentam. A única certeza a ser considerada é a incerteza dos resultados. Segundo Lima (2018), muitos podem considerar a incerteza natural e apostar contra ela em seus planejamentos estratégicos e, dessa forma, lidar com uma projeção de cenário muitas vezes ineficientes.

Com o advento das grandes navegações do século XV, emergiu a necessidade de avaliação dos prejuízos causados pelas perdas dos navios, de forma a quantificar a vantajosidade de uma rota ou de um negócio. Surgia, então, o termo “risco” da forma como conhecemos atualmente, que desde a sua origem está associado à possibilidade de ocorrência de um evento indesejado. Com desenvolvimento da probabilidade, em meados do século XVII, foi possível quantificar estas possibilidades. (Covello; Munpower, 1995, Freitas; Gomez, 1997)

O risco é um conceito fundamental e presente em diversas áreas, desde economia, saúde, segurança e tomada de decisões. Segundo a DCA 16-2 – Diretriz do Comando da Aeronáutica que normatiza a Gestão de Riscos âmbito do Comando da Aeronáutica – o risco é definido como a possibilidade de ocorrência de um evento que venha a ter impacto negativo no cumprimento dos objetivos, sendo mensurado em termos de impacto e de probabilidade. Ampliando este conceito, o impacto de um evento pode não somente ser caracterizado como um aspecto negativo, mas também adquirir perspectiva positiva ou neutra.

Conscientes da existência inevitável do risco, a sua gestão torna-se uma atividade fundamental para as organizações, empresas e indivíduos, envolvendo esforços no sentido de identificar condições potenciais, avaliar sua probabilidade e impactos, evitá-los, mitigá-los ou, sob certas situações, aproveitá-los. Abrange, ainda, um conjunto de ações de boas práticas organizacionais por meio de um constante monitoramento na identificação de novos riscos e da revisão de seu modelo frente a mudanças de cenários.

Considerando as variáveis envolvidas e a evolução dos cenários, o uso de novas ferramentas tecnológicas torna-se fundamental para aprimorar a gestão de riscos nas organizações. A utilização de sistemas integrados que centralizam dados

internos e externos é essencial para a gestão de riscos. Ao ter acesso a informações relevantes provenientes de várias fontes confiáveis e centralizadas em um sistema seguro, os gestores podem identificar, avaliar e monitorar os riscos de forma mais eficiente. A atualização em tempo real e a geração de relatórios precisos contribuem para uma gestão de riscos mais ágil e efetiva, permitindo que as organizações antecipem e mitiguem potenciais ameaças.

Além disso, a utilização de simulações e análises de cenários, proporcionadas por novas ferramentas, possibilita uma avaliação mais precisa dos riscos e de seus impactos potenciais. Isso permite que as organizações desenvolvam planos de contingência mais robustos e tomem decisões mais embasadas para lidar com situações de crise.

Considerando o processo decisório em operações militares, a gestão do risco apresenta-se como um aspecto crucial a ser considerado, pois a capacidade de antecipar e mitigar ameaças pode ser determinante para o sucesso das missões e segurança da tropa.

Segundo Knight (1921), enquanto risco é considerado como uma probabilidade mensurável, a incerteza é uma situação expressa por valores indeterminados e não quantificáveis, isto é, refere-se a uma situação de “probabilidade numericamente imensurável”.

Para Keynes (1937), a natureza epistemológica da incerteza é decorrente do raciocínio indutivo que generaliza decisões baseadas em informações insuficientes e não completamente conhecidas e diz respeito a uma característica do conhecimento dos eventos futuros que, pela natureza intuitiva, não pode ser expresso em termos de uma distribuição de probabilidade quantificável.

Embora tenham sido teóricos com abordagens particulares na área econômica, Keynes e Knight aproximam suas definições para a incerteza quando a caracterizam pela falta de clareza ou certeza sobre eventos futuros, tornando difícil ou impossível estimar com precisão as probabilidades de ocorrência e que está presente em situações em que as informações são limitadas, resultando em um ambiente que desafia a capacidade de qualquer planejamento.

A incerteza pode ser causada por diversos fatores, tais como mudanças inesperadas no ambiente externo, falta de dados confiáveis, complexidade de sistemas envolvidos e interações imprevisíveis entre variáveis. O surgimento de um

dispositivo inovador, uma catástrofe natural, uma epidemia global ou uma brusca mudança política são exemplos de eventos disruptivos que podem gerar incerteza.

Neste contexto, mais uma vez as ferramentas tecnológicas podem contribuir com efeitos minimizadores sobre a incerteza. Em que pese a falta de dados anteriores confiáveis e a possibilidade de ações inesperadas de um oponente militar, o processamento em alta performance conjugado com técnicas de ML e a capacidade de atualização *online* por meio de sistemas tecnológicos de apoio à decisão podem ser uma ferramenta eficaz para quantificação deste cenário, propondo múltiplas alternativas inicialmente ocultas ao decisor, que podem ampliar a sua percepção, intuição, criatividade e capacidade de improvisação, recursos diferenciais e valiosos em um ambiente de incerteza.

3.4 CONFIABILIDADE

O rápido desenvolvimento da IA continua a proporcionar benefícios econômicos e sociais significativos para a sociedade. Sua aplicação em áreas como transporte, finanças, medicina, segurança e entretenimento tem despertado uma crescente conscientização sobre a importância de sua confiabilidade. Isso ocorre porque a quebra de confiança das partes interessadas pode levar a graves consequências sociais, dada a ampla difusão desses sistemas. Por outro lado, os profissionais de IA, incluindo desenvolvedores, programadores e decisores, têm tradicionalmente considerado o desempenho do sistema como a principal métrica nos seus fluxos de trabalho, aspecto longe de ser suficiente para refletir a confiabilidade dos sistemas de IA (Li et al., 2023).

Moubray (2001) define a confiabilidade como a capacidade de um sistema ou componente de realizar suas funções de forma adequada e segura, sem falhas ou defeitos significativos, durante um período determinado.

Considerada um conceito essencial em muitos setores, a confiabilidade está presente desde em sistemas críticos de produção, segurança e engenharia, chegando a produtos e serviços que devem atender às expectativas dos usuários.

A engenharia de confiabilidade é uma área específica que trabalha com a previsão, prevenção, correção e gerenciamento, mesmo em condições de incerteza, de possíveis falhas de material ou sistema por meio de aplicação de técnicas de

análise probabilística, indicando a capacidade de realizar suas funções de forma para a qual foram concebidas. Essas técnicas incluem a modelagem efetiva, análise de ciclo de vida do componente, monitoramento ativo, simulação real ou virtual e a utilização de ferramentas como softwares de análises preditivas.

A fórmula simplificada da confiabilidade é uma ferramenta matemática utilizada para calcular a probabilidade de um sistema ou componente não apresentar falha durante um período específico. A fórmula é baseada na taxa de falhas do sistema, que é a taxa em que o sistema falha por unidade de tempo, conforme abaixo:

$R(t) = e^{-\lambda t}$, onde:

- R(t) é a confiabilidade (do inglês *reliability*) do sistema em uma determinada unidade de tempo t;

- e é o número de Euler, uma constante matemática base dos logaritmos naturais no valor aproximado de 2,71828; e

- λ é a taxa de falhas do sistema, que é a taxa em que o sistema falha por unidade de tempo.

A taxa de falhas do sistema (λ) é calculada dividindo o número de falhas pelo tempo total de operação do sistema. Por exemplo, se um sistema falhou 1 vezes em 10.000 horas de operação, a taxa de falhas seria de 0,0001 falhas por hora.

Para calcular a confiabilidade do sistema em 1.000 horas, você precisaria saber a taxa de falhas do sistema. Se a taxa de falhas for de 0,0001 falhas por hora, você poderia calcular a confiabilidade da seguinte maneira:

Sendo t = 1000 e λ = 0,0001, então $R(1000) = e^{-(0,0001).\ 1000} \approx 0,904837418$

Isso significa que a confiabilidade do sistema em 1000 horas (sua probabilidade de não falhar) é de aproximadamente 90,48%.

O significado deste valor depende da avaliação de criticidade do material ou sistema avaliado. Uma taxa de confiabilidade pode ser aceitável ou adequada para um sistema simples, como um interruptor elétrico para uso residencial, mas pode ser considerado inaceitável para utilização em um sistema crítico, como em um sistema de parada de emergência de um reator nuclear ou em um sistema de armas.

Considerando que medições quantitativas são requisitos determinantes para a engenharia, o desafio para os gestores de TI trata da dificuldade em se estabelecer parâmetros mensuráveis para a confiabilidade de sistemas, os quais podendo variar expressivamente de acordo com o contexto, a criticidade do sistema, dos dados que

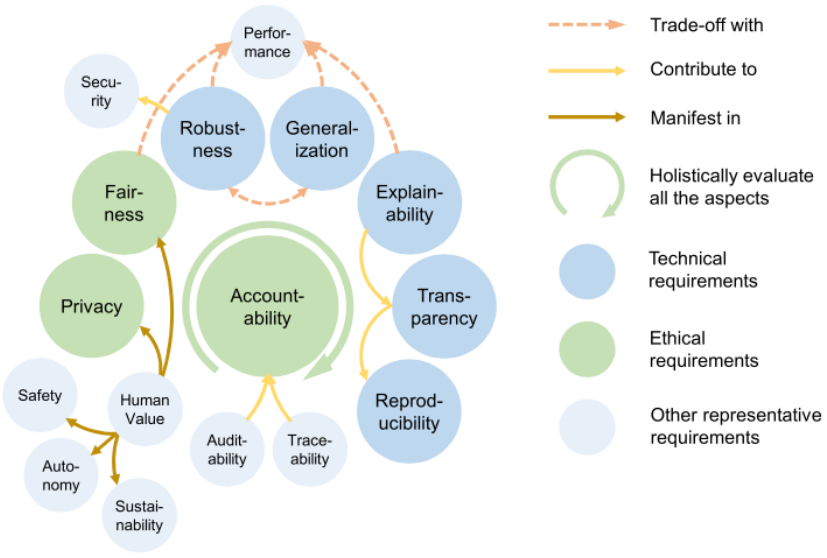
estejam sendo processados, da capacidade de recuperação e de necessidades específicas de cada organização. Em geral, a confiabilidade de sistemas de TI é crucial para garantir a segurança e disponibilidade contínua de serviços e dados, minimizando interrupções e falhas que possam impactar negativamente as operações.

Sommerville (2011) cita que algumas vezes os sistemas computacionais simplesmente “travam” por razões de difícil compreensão ou explicação, ocasionando falhas em disponibilizar os resultados para os quais foram programados.

Com abordagem análoga, Li et al. (2023) conceitua que muitos sistemas são vulneráveis a erros, falhas e ataques imperceptíveis, degradando a experiência e a confiança dos usuários. Neste sentido, requisitos de confiabilidade como robustez, generalização, explicabilidade, transparência, reprodutibilidade, justiça, preservação da privacidade e responsabilidade devem ser abordados de maneira sistemática em todo o seu ciclo de vida, incluindo etapas de preparação de dados, design algorítmico, desenvolvimento e implantação, bem como operação, monitoramento de anomalias, governança e auditoria.

Os diferentes requisitos de confiabilidade de IA possuem interações de dependência, contribuição e *trade-off* [5], apresentados de forma pictorial conforme a figura 7.

Figura 7 - *Trustworthy AI: From Principles to Practices*



Fonte:Li et al., 2023

[5] Conceito que descreve uma situação de escolha entre duas ou mais opções, onde a escolha de uma opção implica a renúncia ou degradação de vantagens da outra.

Requisitos de confiabilidade, suas interações e desdobramentos não são fixos ou plenamente conhecidos e estão em constante evolução. As relações de contribuições destacam-se por proporcionar maior precisão e os *trade-offs* precisam ser muito bem ponderados para cada aplicação específica, devendo ser objeto de monitoramento e governança durante todo o ciclo de vida dos projetos relacionados às novas tecnologias.

3.5 NOVOS DESAFIOS

Neste capítulo foram realizadas considerações acerca da evolução e do potencial transformador da sociedade promovido pelo desenvolvimento tecnológico, apresentando as principais tecnologias da atualidade. Ao conhecer as particularidades de cada tecnologia apresentada e suas interdependências, foi possível identificar uma variedade de aplicações e, entre elas, o grande potencial diferencial de emprego em sistemas de apoio à decisão devido à capacidade de oferecer ferramentas de contorno inerentes aos principais óbices inerentes do processo mental humano apresentados no capítulo anterior.

No entanto, foi também apresentado que o ambiente real infere riscos e incertezas na lógica e no processamento dos sistemas, afetando a sua a confiabilidade. Assim, a implementação de requisitos específicos na sua estruturação constitui elemento essencial e desafiador para a garantia de sua operação confiável, que devem ser objeto de monitoramento e governança durante todo o ciclo de vida dos projetos relacionados, em especial ao tratar de processos que envolvam apoio às decisões militares.

No próximo capítulo serão apresentadas as principais capacidades, desafios e aplicações militares que refletem a tendência do cenário mundial, permitindo a identificação de requisitos de confiabilidade específicos que devem ser observados por todos os *stakeholders*[6] como forma de garantir propostas decisórias equilibradas, eficazes e confiáveis.

---

[6] Constituem organizações, grupos ou indivíduos que possuem interesse, influenciam ou são afetados por atividades e decisões específicas.

4 NOVAS TECNOLOGIAS APLICADAS EM ATIVIDADES MILITARES

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) – adaptação em português para a *Organisation for Economic Co-operation and Development* (OECD) – representa uma estrutura de 36 países membros e outros 5 parceiros estratégicos que discutem políticas públicas para fins do desenvolvimento do bem-estar socioeconômico da população mundial. Como parceiro estratégico e visando o alcance do status de país membro, o Brasil vem aderindo a diversos instrumentos jurídicos, normas e diretrizes propostas pela OCDE.

Para fins de acompanhar os progressos e propor políticas de normatização da implementação de IA confiável, a OCDE desenvolveu o Observatório de Políticas de IA da OCDE (*OECD.AI Policy Observatory*), um ponto central para repositório de dados, análises e relatórios de IA. Dentre os diversos documentos e inciativas, em 2019 a OCDE apresentou, e recentemente (maio/2024) os atualizou, os 10 princípios para a administração responsável de IA. São eles:

– Promover crescimento inclusivo, desenvolvimento sustentável e bem-estar;

– Possuir valores centrados no ser humano e equidade;

– Permitir transparência e explicabilidade;

– Possuir robustez, segurança e proteção;

– Atribuir responsabilidade;

– Investir na investigação e desenvolvimento da IA;

– Promover um ecossistema digital para a IA;

– Criar um ambiente político favorável à IA;

– Reforçar as capacidades humanas e preparar a transformação do mercado de trabalho; e

– Promover a cooperação internacional para uma IA confiável.

Consideradas as tendências da OCDE e do cenário internacional, diversos países estão realizando grandes investimentos no desenvolvimento da infraestrutura e de novas estratégias de emprego da IA. Conforme demonstrado durante a 5ª Conferência Nacional de Ciência, Tecnologia e Inovação, por meio da apresentação da proposta do Plano Brasileiro de Inteligência Artificial (PBIA), o panorama dos investimentos públicos e privados de IA refletem a importância da temática empreendida por alguns países. Além dos valores absolutos investidos e das áreas

de interesse, pode-se observar na tabela 1 a desproporcionalidade dos valores investidos pelos EUA e China.

Tabela 1 – Investimentos públicos de IA no mundo

País	Valores e Descrição
EUA	R$ 63 bilhões de investimentos públicos em P&D de IA (2021-2024) e investimentos privados estimados em 2023 de R$ 380 bilhões
China	R$ 306 bilhões de investimentos públicos *data centers* em 2024 e investimentos privados estimados em 2023 de R$ 39 bilhões
Alemanha	R$ 29 bilhões em 7 anos para investir em 12 campos de ações estratégicas de IA
França	R$ 14 bilhões até 2030 para desenvolver infraestrutura, estabelecer ecossistema de pesquisa e ampliar competitividade industrial em IA
Itália	R$ 6 bilhões em 5 anos para apoiar *startups* e fornecer acesso à infraestrutura de computação de IA
Reino Unido	R$ 18 bilhões em 10 anos para infraestrutura de pesquisa, desenvolvimento de habilidades e criação do AI Safety Institute
União Européia	R$ 16 bilhões (2024-2027) para estabelecer "fábricas de IA" e fomentar aplicação de IA em setores industrias e sociais

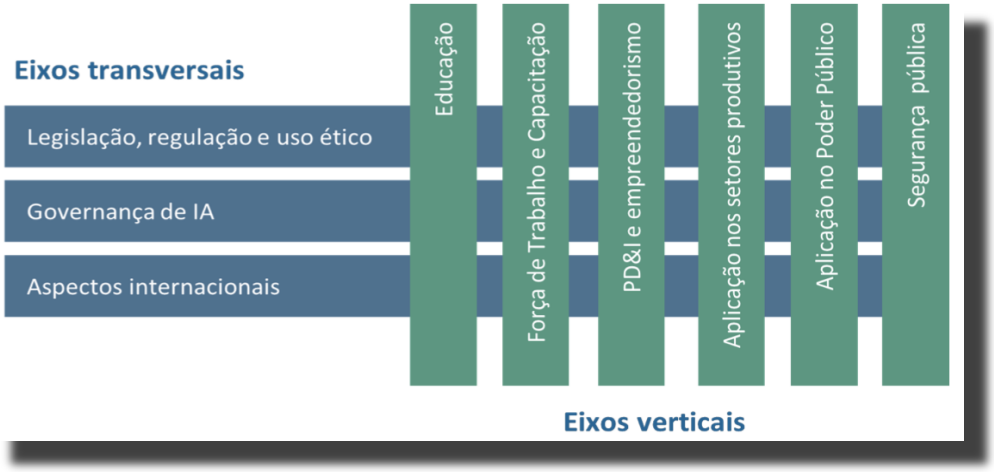
Fonte: PBIA, 2024 (adaptado pelo Autor)

Para fins comparativos, a proposta brasileira prevê um investimento de R$ 23 bilhões em quatro anos e possui direcionamento para as áreas de criação de infraestrutura, desenvolvimento socioeconômico e sustentabilidade. Nota-se ainda, no que denomina como visão do Brasil, considerações sobre a necessidade de autonomia tecnológica, transparência, rastreabilidade e responsabilidade, além de cooperação global baseadas em justiça e benefícios mútuos.

Em termos de ordenamento estratégico para IA, o Ministério da Ciência, Tecnologia e Inovação (MCTI) o estrutura em três eixos transversais caracterizados pela normatização, da ética, da governança e aspectos internacionais, os quais perpassam por seis eixos verticais, definidos como educação, força de trabalho e capacitação, pesquisa, desenvolvimento e empreendedorismo, aplicação nos setores

produtivos, aplicação no poder público e segurança pública, conforme apresentado na figura 8.

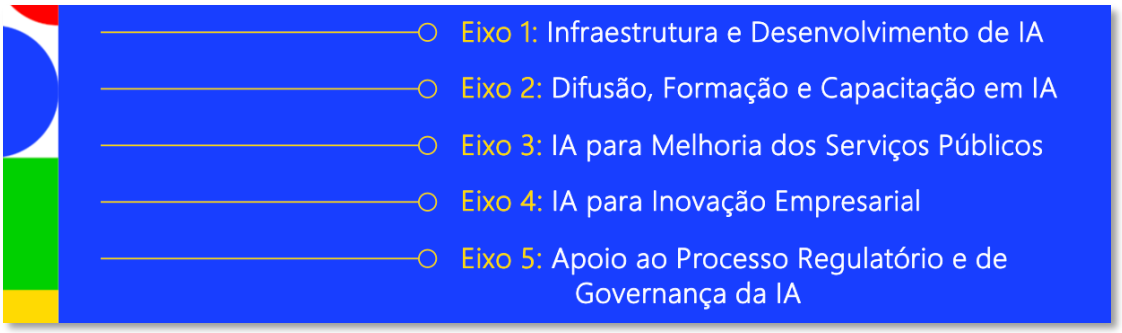
Figura 8 – Eixos da propostas de estratégias



Fonte: MCTI, 2021

A proposta do PBIA, denominada como “IA para o bem de todos”, demonstra forte preocupação com a acessibilidade e apresenta um novo modelo baseado na definição de 6 eixos estruturantes, conforme demonstrado na figura 9, os quais possuem uma lista de ações específicas.

Figura 9 – Eixos estruturantes do PBIA



Fonte: Proposta do PBIA, 2024

Mesmo sendo a tecnologia um fator sempre presente e protagonista nas campanhas militares, proporcionando avanços significativos em termos de eficiência, segurança e precisão, além de ser elemento motriz de profundas discussões éticas e legais, não é explicita a definição política, técnica, normatizadora e de investimentos públicos que tratem, especificamente, do fomento ao emprego militar da IA, seja nos princípios apresentados pela OCDE como pelos eixos estruturantes do PBIA, os quais

se alinham nas áreas de estudos e investimentos realizados pelos países, os quais demonstram focar em abordagens nos aspectos socioeconômicos e industriais.

No entanto, a relevância do tema e suas potencialidades de emprego militar não é negligenciada pelos centros de pesquisa dos países de primeiro mundo. Em 2018, a *Defense Advanced Research Projects Agency* (DARPA) publicou a *Special Notice* 18-80, apresentando as aplicações da IA no processo de tomada de decisão militar como uma oportunidade disruptiva, que podem incluir desenvolvimento de novas estratégias, planejamento de curso de ação, análises táticas em tempo real, coleta de inteligência, jogos de guerra e simulação, detecção de engano, formação e evolução de coalizões.

No campo político, a *National Defense Strategy* (2022) americana destaca a tecnologia como fator diferencial da vantagem militar dos EUA ao longo da história, citando diretamente a aplicação da IA confiável e de sistemas autônomos como capacidades militares atuais relevantes e destacando sua aplicação em operações conjuntas e na otimização no emprego dos meios.

Diante das possibilidades que as novas tecnologias podem proporcionar, as aplicações no campo militar merecem um destaque especial. Devido ao seu potencial de transformar profundamente desde o emprego tático até o planejamento estratégico militar, por meio da ampliação das capacidades já existentes ou desenvolvimento de novas possibilidades com aplicações em diversos domínios e permitindo a execução de missões complexas de forma conjunta, com maior eficiência, eficácia e a segurança operacional, as novas tecnologias constituem uma verdadeira revolução nos assuntos militares[7] a ser explorada. Uma consolidação das capacidades e possibilidades de emprego militar serão apresentadas no Apêndice A.

4.1 DECISÕES MILITARES SUPORTADAS POR SISTEMAS INTELIGENTES

Segundo Williams (2011), a volatilidade, a incerteza, a complexidade e a ambiguidade do ambiente operacional militar exigem decisões rápidas em situações em que os processos decisórios consagrados são limitados ou ineficazes.

---

[7] Conceito que trata da teoria do futuro da guerra, que se refere a uma nova ideia, procedimento, sistema ou equipamento cujos efeitos promovem uma profunda mudança na maneira atual de pensar ou agir sobre algo, podendo alterar doutrinas militares nos níveis estratégicos, operacionais ou táticos.

Riscos e incertezas podem ser fatores especialmente críticos em um processo decisório militar, pois as decisões tomadas podem ter consequências graves e irreversíveis. Neste sentido, a utilização de ferramentas que ampliem a capacidade de decisão e minimizem as heurísticas e vieses inerentes ao processo cognitivo humano, podem ser determinantes para a vida humana ou o destino de uma nação.

Um exemplo catastrófico de uma decisão militar errada ocorreu em 3 de julho de 1988, quando uma aeronave comercial modelo Airbus 300, efetuando o voo 655 da empresa Iran Air e com 290 pessoas a bordo, foi abatida por dois mísseis lançados pelo *United States Ship* (USS) Vincennes, equipado com o sistema Aegis[8], que operava no Golfo Pérsico em meio ao conflito entre o Irã e o Iraque. A investigação, realizada pelo *U.S. Department of Defense* (Departamento de Defesa Americano - DoD), concluiu que os dados fornecidos pelo sistemas Aegis estavam operacionais e corretos, porém a interpretação do Comandante e a tripulação foi dissonante, decorrente de um conjunto de fatores que induziram a um processo denominado como ilusão cognitiva. Caso as atuais funcionalidades de reconhecimento de padrões baseados em IA e *Big Data*, em conjunto com a integração de dados com sistemas de controle de tráfego aéreo e outros recursos de apoio à decisão, estivessem disponíveis à tripulação naquele evento, a consciência situacional estaria ampliada com as novas informações relevantes, que poderiam produzir efeitos mitigatórios ao processo de ilusão cognitiva ou, até mesmo, criar mais uma barreira de verificação e validação no sistema de acionamento dos mísseis, evitando-se a perda de 290 vidas inocentes.

Em termos de decisão estratégica, um exemplo por meio do qual as novas tecnologias de apoio à decisão poderiam ter alterado o rumo da história foi a Operação Barbarossa, que consistiu na invasão da Alemanha Nazista à União Soviética, em 1941. Os atuais pensadores militares consideram que ocorreram decisões estratégicas erradas as quais poderiam ter sido evitadas ou mitigadas pelas atuais ferramentas preditivas e de simulação de cenários, incluindo a subestimação da capacidade de resistência soviética, as dificuldades logísticas devido a não ponderação adequada sobre extensão do território a ser conquistado, a incorreta

---

[8] Sistema de armas naval centralizado, automatizado, de comando e controle (C2) e controle de armas, projetado como um sistema de armas completo, desde a detecção até a eliminação, desenvolvido pela empresa Lockheed Martin.

avaliação climática do rigoroso inverno russo e a decisão de dividir as forças alemãs em múltiplas frentes de combate. O resultado foi um desastre retumbante para ofensiva alemã com grandes perdas humanas e materiais, considerado como o início da sua derrocada na Segunda Guerra Mundial.

O emprego de algumas das capacidades e aplicações apresentadas pode ser observado no atual conflito entre Rússia e Ucrânia, iniciado em fevereiro de 2022, por meio do emprego massivo de drones remotamente pilotados ou autônomos, realizando desde missões de reconhecimento ao emprego de armamentos. Um aspecto relevante a se observar, trata da assimetria da capacidade bélica dos países envolvidos e o relativo sucesso dos meios considerados mais “fracos” militarmente, porém dotados de mais “inteligência”. A figura 10 demonstra uma imagem de um momento anterior a um exitoso emprego de um drone naval ucraniano de baixo valor sendo utilizado contra um moderno navio de guerra russo.

Figura 10: Drone naval Ucraniano em rota de ataque

Fonte: https://youtu.be/GDDfNNmTHOc. Acesso em: 12 jun. 2024

O emprego de drones equipados com sensores de reconhecimento, armamentos inteligentes e capacidade de comunicação de dados em rede segura, que podem operar em condições meteorológicas adversas, tanto em ambiente diurno quanto noturno, amplia sobremaneira o nível de consciência situacional do cenário e racionaliza o emprego das capacidades bélicas de seus operadores. Ao mesmo tempo em que é empregado em uma missão de ataque, o drone pode realizar a avaliação de danos e atualizar o cenário do campo de batalha, permitindo que o processo decisório sobre os efeitos ou necessidades para novas surtidas seja atualizado em

tempo real. Na figura 11, pode ser visualizado o drone de origem turca Bayraktar TB2, utilizado pela Ucrânia, equipado com diversos sensores e armamentos.

Figura 11 – Drone Bayraktar TB2

Fonte: https://www.navalnews.com/naval-news/2022/05/surprising-success-of-ukraines-bayraktar-tb2-the-ghost-of-snake-island/. Acesso em: 13 jun. 2024

Entretanto, no Brasil, o Ministério da Defesa (MD) e as FA ainda não possuem uma estratégia unificada e integrada para exploração das capacidades de tais tecnologias, criando a possibilidade da existência de lacunas tecnológicas ou sobreposição de esforços. Por exemplo, a Marinha do Brasil (MB) e o Exército Brasileiro (EB) desenvolveram, por meio de iniciativas isoladas e empregando recursos distintos, sistemas de *chatbot* [9] administrativos que possuem arquiteturas e funcionalidades diferentes. Já a Força Aérea Brasileira (FAB), que ainda não dispõe de tais ferramentas, está envidando esforços no desenvolvimento de sistemas de IA nas áreas de gestão de documentos e de logística de materiais, áreas comuns às demais FA e que não estão sendo desenvolvidas em conjunto com as demais FA.

Ao se constatar este cenário, em que sistemas tecnológicos com funcionalidades de suporte à decisão estão sendo desenvolvidos por meio de inciativas próprias de cada FA, faz-se determinante a busca pela harmonização da padronização de suas estruturas, em especial os requisitos de confiabilidade, de

[9] Algoritmos utilizados para simular a conversa humana, capazes de interagir, automaticamente, usando inteligência artificial e técnicas de aprendizagem de máquina. São utilizados para a resolução de dúvidas e para o provimento de determinadas informações solicitadas pelo usuário.

forma que os sistemas possam ser futuramente utilizados em ambientes distintos, mas de forma interoperável, com segurança técnica e operacional.

4.2 CONFIABILIDADE EM SISTEMAS DE APOIO À DECISÃO

A utilização operacional e comercial de um novo produto ou sistema é precedido por um processo denominado como certificação, um procedimento formal composto de conjunto de testes segundo protocolos e critérios específicos, efetuada por entidades certificadoras competentes, que garantem o cumprimento dos requisitos de confiabilidade, qualidade e conformidade operacionais mínimas de forma consistente, segura e precisa.

Em se tratando do emprego para fins militares, podem ser exigidos parâmetros mais restritivos do que os utilizados para os de fins comerciais, tais como uma maior robustez para o funcionamento em condições adversas, funcionalidade de proteção eletrônica frente a interferências ilícitas ou possuir uma bateria com maior duração e tempo de recarga reduzido.

A maioria dos trabalhos acadêmicos está centrado no desenvolvimento das capacidades de desempenho algorítmico, os quais são insuficientes para abrangerem os aspectos relacionados à confiabilidade. Li et al. (2023) destaca que, do ponto de vista industrial, o ciclo de vida de um sistema inteligente possui vários estágios, incluindo sanitização de dados, desenvolvimentos de design algorítmico robustos, monitoramento de anomalias, governança e auditoria. Melhorar a confiabilidade envolve esforços sinérgicos e em vários momentos deste ciclo de vida. Em contrapartida, a quebra de confiança em qualquer etapa ou aspecto pode prejudicar a confiabilidade de todo o sistema.

A criticidade dos impactos resultantes do processo decisório no ambiente militar impõe o amplo domínio e o estabelecimento de requisitos de confiabilidade bem definidos, de forma a garantir que os algoritmos sejam corretos, justos, éticos e livres de vieses, oferecendo segurança e autonomia ao decisor no gerenciamento eficaz dos riscos e das incertezas.

Considerando os conceitos apresentados, desde as limitações do processo mental cognitivo, suas sujeições à heurísticas e vieses, as novas tecnologias disponíveis e suas aplicações no campo militar, foi identificada a existência de uma

condição de equilíbrio estático instável na confiabilidade de novos sistemas de apoio à decisão, a qual é sustentada por um conjunto de requisitos críticos que se interrelacionam entre si e obtiveram maior prevalência ao longo deste trabalho, caracterizados pela Transparência Algorítmica, Explicabilidade, Interoperabilidade, Robustez, Redundância e Responsabilidade. Cumpre destacar a existência de outros requisitos, porém considerados de menor relevância para fins deste trabalho.

Li et al. (2023) destaca a importância para a combinação e interação entre os requisitos associados à confiabilidade. Por exemplo, a responsabilidade referente à privacidade dos dados pode interferir na explicabilidade do sistema, e a busca pela interoperabilidade pode ser prejudicial à robustez. Neste sentido, a somatória trivial para fins de melhorar separadamente cada aspecto da confiabilidade não garante um resultado mais confiável e eficaz. Em vez disso, são necessárias otimizações conjuntas e compensações entre múltiplos aspectos de confiabilidade, sugerindo uma abordagem sistemática para mudar o paradigma do *trade-off* entre os requisitos. Isto requer um elevado nível de cooperação das partes interessadas em diferentes fases do ciclo de vida do sistema.

4.2.1 Transparência Algorítmica

O conjunto de procedimentos que visam tornar visíveis e formalmente documentadas todas as etapas dos processos realizados, a base de dados empregada, as decisões implementadas e a quantificação das ponderações adotadas, permitindo que especialistas e demais partes interessadas possam auditar e entender todo o processo, define o conceito de transparência algorítmica. Constitui-se como requisito fundamental para construir a confiança nos sistemas automatizados, permitindo a identificação da lógica e das limitações cognitivas, das heurísticas e vieses descritas no segundo capítulo, além de garantir uma operação baseada em parâmetros de justiça e ética, ajudando a prevenir, mitigar ou corrigir possíveis erros, deliberados ou não, nas soluções que venham a ser apresentadas.

O *design* de algoritmos transparentes deve pautar-se em modelos providos de metadados[10], apresentando a fonte dos dados, a data de coleta, o método de

[10] Refere-se a um conjunto de dados que fornecem informações detalhadas sobre outros dados, de forma a localizá-los, entendê-los, utilizá-los e gerenciá-los.

processamento, interações humanas realizadas e outras informações customizáveis de interesse. Ademais, deve possuir capacidade de armazenamento como forma de registro documental para ações de governança e auditora. A somatória desses dados deve ser suficiente para apresentar de forma inequívoca a justificativa do resultado obtido de todo o processamento.

Li et al. (2023) denota a tendência atual da utilização de sistemas de código aberto como metodologia que contribui significativamente para a transparência algorítmica dos sistemas, abordando que sua abrangência deve contemplar a multiplicidade de possíveis cenários e o registro da dinâmica de eventos realizados. No entanto, esta abordagem deve ser amplamente ponderada pelos desenvolvedores de sistemas militares, pois o relativo ganho na transparência algorítmica com a utilização do código aberto pode consistir em um ponto intrínseco de vulnerabilidade para ataques maliciosos.

Um recurso técnico que pode ser utilizado para mitigar os riscos associados ao uso de código aberto em sistemas militares consiste na utilização de um *design* de segmentação em camadas, permitindo que partes do sistema sejam verificados sem expor partes críticas e com informações sensíveis do código-fonte, deixando-as ocultas ou com acesso restrito. Ao segmentar a transparência em camadas, aspectos menos críticos permanecem acessíveis para auditorias e melhorias colaborativas, equilibrando a necessidade de segurança com os benefícios da transparência e da colaboração aberta.

Em sistemas decisórios militares, embora seja benéfica em termos de responsabilidade, a transparência algorítmica pode representar um risco de exposição de dados sensíveis referentes às estratégias e táticas empregadas, tornando-se uma vulnerabilidade com potencial de exploração adversária. Ademais, pode afetar a legitimidade dos atos em questionamentos e litígios jurídicos futuros, suscitando dilemas éticos complexos ao transparecer em suas programação as regras que podem tomar decisões de vida ou morte.

Neste sentido, é recomendável que sistemas decisórios para emprego pelas FA sejam produtos resultantes de desenvolvimento autóctone, possuam metadados customizáveis e que adotem equidade de parâmetros de segurança e eficácia operacional, assim como adotar estratégias específicas de mitigação, como a limitação da transparência para somente a partes interessadas de alto nível.

4.2.2 Explicabilidade

A explicabilidade é definida como a capacidade de fornecer informações compreensíveis, de forma clara, objetiva e que alcance até os usuários finais, da lógica de programação adotada para se chegar a uma decisão ou resultado específico de um processamento, com registro integral das operações realizadas, podendo se apresentar em forma de uma narrativa descritiva ou de visualizações pictoriais.

Li et al. (2023) orienta a explicabilidade de um modelo por meio da avaliação de sua entrada, do resultado intermediário e a saída final. Para explicar o comportamento de um sistema que utiliza ML com rede neural de múltiplas camadas, recomenda a inspeção dos recursos intermediários, ou seja, aplicar a explicabilidade para o resultado de cada camada de processamento da rede. Sempre que possível ou aplicável, ao utilizar modelos de ML é desejável que utilizem modelos que sejam mais facilmente interpretáveis, como árvores de decisão e regressões lineares.

Os métodos de explicabilidade devem possuir amplitude local - métodos que expliquem decisões individuais do modelo, tais como LIME (*Local Interpretable Model-agnostic Explanations*) ou SHAP (*SHapley Additive exPlanations*) - e global, que forneçam o detalhamento sobre o comportamento geral do modelo e de *compliance* ao objetivo estabelecido. A utilização de *dashboards* de monitoramento em tempo real apresenta-se como uma importante ferramenta para desenvolvedores e decisores, permitindo ações corretivas quando a temporalidade permitir, além de fornecer indicadores de performance e dados de governança.

Neste momento, faz-se importante esclarecer que, embora sejam conceitos relacionados na medida em que visam aumentar a compreensão e a confiança nos sistemas, transparência algorítmica e explicabilidade são conceitos distintos. Enquanto a transparência algorítmica abrange uma visão completa e profunda do funcionamento interno do algoritmo, incluindo dados, código, processos e parâmetros, sendo direcionada a especialistas, desenvolvedores, auditores e *stakeholders* técnicos, a explicabilidade visa proporcionar o entendimento mais claro e compreensível sobre decisões tomadas pelo algoritmo, muitas vezes simplificando ou abstraindo detalhes técnicos, sendo direcionada para usuários finais e *stakeholders* não técnicos e utilizando narrativas simplificadas, visualizações e técnicas *pós-hoc* para explicar decisões específicas de maneira intuitiva e acessível.

Conjugada com a transparência algorítmica, a implementação da

explicabilidade em decisões militares não só melhora a eficácia operacional, mas também assegura que as ações sejam tomadas de forma responsável, ética e em conformidade com leis e convenções, tanto nacionais quanto internacionais, mantendo a confiança dos usuários e a legitimidade das FA perante toda sociedade e a comunidade internacional.

4.2.3 Interoperabilidade

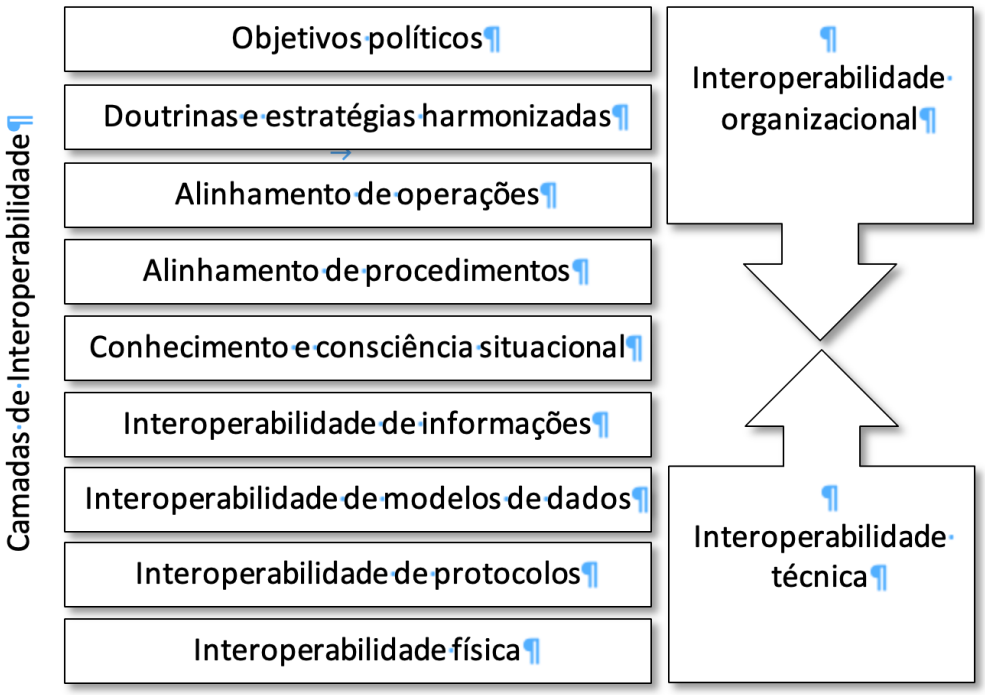
Segundo a Escola Nacional de Administração Pública (ENAP), interoperabilidade refere-se à capacidade de diversos sistemas, dispositivos e organizações trabalharem em conjunto para trocar informações de maneira eficaz e eficiente. Para a sua exequibilidade é necessário que seja utilizada em linguagem mutuamente compreensível, utilizável e colaborativa, ampliando as suas capacidades individuais.

Tolk (2003) propôs um modelo conceitual de interoperabilidade composto de um conjunto de nove camadas que são categorizadas em dois grupos, denominados organizacional e técnico. O conceito de interoperabilidade organizacional relaciona-se com a coordenação de objetivos políticos, harmonização de doutrinas e estratégias, alinhamento de metodologias operacionais e procedimentos e um ambiente colaborativo. Sobre a interoperabilidade técnica, seu modelo apresenta as camadas de troca de informações, modelagem de dados, protocolos e dispositivos físicos, conforme apresentado no modelo simplificado de Tolk da figura 12.

A principal contribuição do modelo de Tolk não está em atribuir grau de importância das camadas, mas na constatação de que a deficiência em uma camada pode comprometer o desempenho da outra e, por conseguinte, desestruturar a interoperabilidade sistêmica global.

Observando-se as camadas técnicas verifica-se que os riscos associados estão diretamente relacionados à incompatibilidade de protocolos, formatos de dados e falta de padronização de interfaces de comunicação, podendo inviabilizar a troca de informações ou escalabilidade entre plataformas ou sistemas diferentes.

Figura 12 – Modelo de interoperabilidade de Tolk



Fonte: Tolk, 2003 (adaptado pelo Autor)

Sendo a interoperabilidade dos sistemas de apoio à decisão fundamental para garantir a coordenação do emprego em operações conjuntas das FA, as ferramentas tecnológicas empregadas devem possuir estruturas orientadas por satisfazer as camadas da interoperabilidade técnica de Tolk. Assim, é recomendável que o desenvolvimento de qualquer sistema que se vislumbre a possibilidade de emprego conjunto, seja administrativo ou operacional, tenha a participação de especialistas técnicos de cada FA, evitando-se iniciativas isoladas que podem comprometer a possibilidade de uma futura interoperabilidade ampla.

Em outra abordagem, dados insuficientes ou inconsistentes podem induzir falhas ou gerar resultados inadequados. Neste sentido, a interoperabilidade de dados – podendo abranger, inclusive, interoperabilidade em *Big Data* – entre sistemas de cada FA constitui uma ferramenta que, além de aumentar a base de dados por meio de outra fonte confiável, permite a execução de validação cruzada de utilidade para ambos os sistemas que os compartilham. Segundo Tonin (2019), a lacuna de IA da tecnologia de defesa entre os aliados deve permanecer pequena o suficiente para ser preenchida pela interoperabilidade. Tal abordagem promove maior resiliência por meio de redundância em caso de falhas e garante aumento da robustez na precisão

e qualidade dos dados, requisitos de confiabilidade que serão detalhados ainda neste capítulo.

Para fins de mitigar uma possível falta de padronização de protocolos, o desenvolvimento de APIs[11] (*Application Programming Interfaces*) pode representar uma solução técnica. No entanto, tal prática, além de complexa, pode representar novos custos e afetar o desempenho geral, pode induzir novos erros sistêmicos e abrir oportunidades de violações de segurança não desejáveis para sistemas militares. Mais uma vez, o desenvolvimento conjunto mostra-se como a solução mais adequada.

Garantir que sistemas sejam interoperáveis não se trata de um *trade-off* entre perda de poder decisório ou autonomia, mas de uma evolução da cultura do processo decisório que requer um esforço contínuo de desenvolvimento, quebra de paradigmas organizacionais, implementação de normas conjuntas, execução de testes rigorosos e capacitação de pessoal. A adoção da interoperabilidade em sistemas de apoio à decisão pode melhorar significativamente a capacidade das FA em tomar decisões mais eficientes e coordenadas, contribuindo para a segurança e a eficácia das operações conjuntas.

4.2.4 Robustez

O conceito de robustez remete à ideia de senso comum de um produto resistente e durável. No entanto, em termos algorítmicos ou sistêmicos, Li et al. (2023) a define como a capacidade de lidar com erros de execução, de entrada de dados errados ou insuficientes, evitando-se um comportamento não esperado. Frisa-se, ainda, sobre a criticidade deste requisito em aplicações de alto risco devido ao seu impacto direto na segurança e proteção dos resultados obtidos.

Em termos de sistemas decisórios e aplicações militares, a robustez torna-se fundamental para a garantia da operacionalidade em condições adversas e dinâmicas, com dados ruins ou incompletos, ataques maliciosos ou falhas de componentes.

Para contornar os desafios referentes aos dados, sejam ruins ou insuficientes, o uso do *Big Data* confiável associado a uma capacidade de generalização controlada

---

[11] Aplicativos que permitem a comunicação de dados e funcionalidades entre diferentes sistemas de software, facilitando a interoperabilidade entre sistemas diferentes.

de cenários similares – técnicas consolidadas de ML – consistem em eficientes soluções práticas e aplicáveis.

A contraposição a ataques adversários com intenções maliciosas é um dos maiores desafios para sistemas, pois as ações ofensivas podem possuir origem em diversas fontes. Basicamente, o ideal é que todos os componentes de um sistema crítico sejam interconectados em rede própria e segura, além de adotar um rigoroso mecanismo de controle de acesso e com separação de níveis das camadas de processamento e das partes interessadas. Ademais, a utilização de ferramentas de validação cruzada em diferentes subconjuntos de dados e do monitoramento de comportamento anômalo podem resultar em eficazes soluções técnicas, que também devem ser objeto de explicabilidade.

Em termos físicos, a falha de componentes deve ser uma preocupação constante em sistemas tecnológicos durante todo o ciclo de vida, pois afeta direta e visivelmente a funcionalidade do sistema. No entanto, falhas acidentais ou intencionais decorrentes de programações ocultas em nível de processadores podem ser imperceptíveis, representando uma ameaça a sua confiabilidade. As vulnerabilidades mais conhecidas são os *backdoors*[12], *firmwares*[13] maliciosos, *trojan*[14] em processadores e *rootkits*[15] de hardware.

O desenvolvimento autóctone representa a solução técnica ideal, no entanto poucos fabricantes mundiais dominam a tecnologia de produção de circuitos integrados, representando uma dependência e um risco global a ser gerenciado por todos, por meio de execução de auditorias de segurança, transparência dos fornecedores e atualizações constantes.

A implementação e a manutenção da robustez em sistemas de apoio à decisão é um desafio contínuo que envolve a aplicação conjunta de técnicas e abordagens específicas para garantir a sua operação confiável em cenários incertos, sujeitos à falhas e, principalmente, ameaças externas.

---

[12] Falhas ou procedimentos ocultos que contornam processos de autenticação, permitindo acesso remoto não autorizado.

[13] Programas de baixo nível que controlam o funcionamento básico de um *hardware*.

[14] Códigos ocultos maliciosos que podem ser inseridos em programas ou em circuitos integrados durante o processo de fabricação.

[15] Programas maliciosos que se instalam em nível de sistema operacional, de difícil identificação e remoção.

4.2.5 Redundância

O conceito de redundância refere-se à utilização de componentes ou sistemas trabalhando em paralelo e sincronizados de modo que, em caso de uma falha, o outro possa assumir suas funções sem degradação funcional ou perda da continuidade operacional, requisitos essenciais para garantir a eficácia e a confiabilidade das operações militares. No entanto, a redundância pode também inferir o conceito de sobreposição de atividades ou morosidade devido processos desnecessários, induzindo custos administrativos, logísticos ou operacionais.

Para fins deste trabalho, o conceito de redundância possui aderência ao requisito de robustez de sistemas, sendo abordado como um aspecto determinante para a salvaguarda do funcionamento sem solução de continuidade e confiabilidade dos sistemas de apoio à decisão militar.

Ao descrever a Comparação de Poderes de Combate (CPC), a Doutrina de Operações Conjuntas – MD30-M-01/Volumes 1 e 2 (2ª Edição/2020) aborda o emprego de ferramentas de apoio à decisão nas funções de Comando e Controle (C2) como forma de permitir uma análise do exame das forças inimigas e das próprias forças, por meio da utilização de sistemas com capacidade de redundância e contingência. Realiza, ainda, considerações acerca da correlação entre a redundância e a interoperabilidade de sistemas nas FA, segundo o qual propõe o emprego de dados de elos de inteligência e do banco de dados unificado dos Centros de Inteligência de Força de forma compartilhada e interoperável, funcionando como um sistema contingencial, de forma que não haja solução de continuidade das operações militares que dependam dos sistemas envolvidos.

Considerando a arquitetura de sistemas, a redundância deve permitir a somatização de entrada de dados entre diferentes fontes, aumentando a precisão, variabilidade e amplitude das informações disponíveis. Essa verificação é fundamental para evitar erros com dados dinâmicos, que podem ter consequências graves em operações militares. Um outro artifício técnico, consiste na validação cruzada por níveis de camadas algorítmicas, identificando resultados anômalos em etapas anteriores ao final do processo e possibilitando correções antes do processamento decisório final. Com efeito, para que seja executada, identifica-se a necessidade de implementação dos requisitos de transparência algorítmica e da explicabilidade, também abordados anteriormente.

Não menos importante, a infraestrutura física que fornece suporte ao funcionamento dos equipamentos também deve ser considerada para fins da garantia da continuidade de funcionamento de sistemas críticos. Neste sentido, podem ser adotados sistemas redundantes de *hardware*, de comunicação, de sensores e de energização, onde a relação custo-benefício deve ser observada sobre a ótica de risco-criticidade para a sua implementação. Como exemplo, considerando a criticidade da circulação geral do tráfego aéreo nacional, o Sistema de Gerenciamento de Movimentos Aéreos[16] (SIGMA), desenvolvido sob requisitos definidos e operado pela FAB, possui redundância física de todo o sistema disposto em localidades distintas, possuindo redundância de energização elétrica em cada localidade, dualidade em redes de comunicação e de dados, operando de maneira síncrona e com chaveamento automático.

A redundância em sistemas de apoio à decisão militar constitui uma estratégia essencial para a minimização dos riscos associados a possível falhas de sistemas críticos, assegurando que as informações necessárias estejam sempre disponíveis para os níveis decisores.

4.2.6 Responsabilidade

Dentre os diversos requisitos estruturais para a concepção de um sistema confiável apresentados neste trabalho, a responsabilidade trata da conceituação de deveres e garantias para sua utilização ética, justa e segura, gerenciando riscos associados desde discriminação algorítmica, invasão de privacidade a decisões autônomas, afetando, em diferentes níveis, indivíduos e organizações que desenvolvem, implantam, monitoram e o utilizam durante todo o ciclo de vida, buscando identificar eventuais desvios ou falhas comportamentais, sejam erráticas ou intencionais.

Segundo Li et al. (2023), a responsabilidade exige que as partes interessadas sejam obrigadas a justificar a concepção, implementação e operação alinhadas com os valores humanos, sendo concretizada por um design de arquitetura técnica

---

[16] Consiste em uma plataforma integrada para o gerenciamento de informações, processo decisório e operações de tráfego aéreo, funcionando ininterruptamente e integrando uma ampla variedade de sistemas (radares, comunicações e navegação) e de gestão de informações de voo.

confiável, uma avaliação responsável dos impactos potenciais e a divulgação de informações sobre esses aspectos. Esta abordagem, possui relação direta com os requisitos de transparência algorítmica e explicabilidade, permitindo a sua auditabilidade.

Como uma ferramenta de apoio à decisão e não como uma autoridade final, os usuários devem ser capazes de questionar e entender as recomendações do sistema. Assim, a compreensão clara das atribuições, dos níveis de competências e das garantias individuais são condições determinantes para a justa responsabilização em caso de falhas ou decisões incorretas. Usuários finais devem ser bem treinados para entender como o sistema funciona, a sua conformidade legal e regulamentar, quais são suas limitações e como interpretar suas recomendações.

Em outra perspectiva, a adoção de mecanismos de autoproteção de competências, de decisões anômalas e de barreiras múltiplas de verificação em função da criticidade da decisão são condicionantes de proteção que podem ser incorporados na própria estrutura algorítmica do sistema.

O emprego de sistemas autônomos, em particular LAWS, têm suscitado desafios sobre a responsabilização e profundos questionamentos em aspectos éticos e morais. Neste caso, a decisão final para o emprego de um armamento que poderá causar a perda de vidas humanas é tomada, de forma independente, pelo algoritmo.

A regulamentação e o desenvolvimento de normas legais específicas são determinantes para a segurança e a responsabilidade de todas as partes interessadas. Considerando que não existe consenso ou tratado no âmbito do Direito Humanitário Internacional (DIH) sobre a responsabilização no emprego de LAWS, seja para desenvolvedores ou decisores em fase imediatamente anterior ao engajamento autônomo, diversas iniciativas estão sendo discutidas em fóruns internacionais, como a ONU e a União Europeia. No entanto, a possibilidade de um regramento internacional de maneira análoga ao Tratado de Não-Proliferação de Armas Nucleares[17] (TNP) poderá garantir às nações já detentoras das novas tecnologias uma vantagem competitiva assimétrica e impor dificuldades ou restrições aos demais países que buscam o seu desenvolvimento.

---

[17] Refere-se ao acordo internacional que visa prevenir a disseminação de armas nucleares, promover a cooperação no uso pacífico da energia nuclear e avançar no desarmamento nuclear.

No Brasil, encontra-se em tramitação no Senado Federal o Projeto de Lei nº 2.338/2023 que dispõe das regras gerais para o desenvolvimento, a implementação e o uso responsável de sistemas de IA, tendo como um dos objetivos a implementação de sistemas seguros e confiáveis. Em sua justificativa, denota a valorização da proteção dos direitos sociais e garantia das liberdades individuais, apresentando um texto regulatório baseado em gestão de riscos e modelagem fundamentada em direitos. No entanto, a proposta carece de elementos específicos que considerem o emprego militar e sua relevância para aspectos que se relacionam com a defesa nacional, sob pena de poder constituir um limitador legal para o desenvolvimento de potencialidades diferenciais no campo de batalha, tais como SNT e LAWS.

A definição dos critérios de responsabilidade é um componente crucial da confiabilidade dos sistemas de apoio à decisão. Ela abrange a ética no desenvolvimento, a segurança na implementação, o uso informado e a conformidade com normas e regulamentos nacionais e internacionais. Ao garantir que todas essas áreas sejam abordadas, a responsabilidade contribui para a criação de sistemas de apoio à decisão que são justos, transparentes e confiáveis.

5 CONCLUSÃO

Esta pesquisa teve como objetivo analisar os principais requisitos que sustentam a confiabilidade das arquiteturas de sistemas de apoio ao processo decisório militar que empregam novas tecnologias.

O estudo abrangeu desde o modelo do processo mental humano e as teorias clássicas do processo decisório até as características e capacidades das novas ferramentas tecnológicas, destacando a importância de sua integração para aplicação confiável em cenários complexos e dinâmicos sujeitos à riscos e incertezas.

A revisão das teorias do processo decisório destacou a complexidade e a diversidade dos modelos que buscam explicar como decisões são tomadas, apresentando que a integração dessas teorias com novas tecnologias pode potencializar a eficácia dos sistemas de apoio à decisão.

O reconhecimento de que os decisores humanos operam sob limitações cognitivas e temporais – conceito da racionalidade limitada – reforçaram a percepção de que sistemas inteligentes podem fornecer suporte decisório com base de dados mais amplos e em tempo real. Já a combinação de abordagens normativas – como a teoria da utilidade esperada – com abordagens descritivas que consideram as heurísticas e vieses associadas às considerações de que decisões muitas vezes são iterativas e adaptativas, indicam que os sistemas de apoio à decisão devem ser flexíveis e capazes de evoluir com o tempo e com novas informações.

Ao examinar a evolução tecnológica foi possível identificar seus efeitos transformadores que foram capazes de induzir profundas mudanças no ambiente, moldar novos comportamentos sociais e impulsionar o desenvolvimento de outras áreas de conhecimento. Foi apresentado que ferramentas tecnológicas avançadas, como *Big Data*, Inteligência Artificial, *Machine Learning* e *Deep Learning* descortinam novas possibilidades na análise de grandes volumes de dados, estruturados ou não, permitindo a identificação de padrões ocultos, realizando predições de resultados ou de ações adversas, além de possuir a capacidade de fornecer recomendações adaptativas com atualização em tempo real, constituindo-se como inovações disruptivas para o processo decisório.

Nesta abordagem, por meio de conceituações teóricas sobre risco e incerteza, verificou-se que a tecnologia desempenha um papel crucial na gestão e mitigação desses desafios, especialmente em operações críticas como as militares. O emprego

de sistemas de IA conjugados com técnicas de aprendizado de máquina permitem análise em tempo real e simulações com alta precisão, auxiliando no processo de tomada de decisões. Assim, verificou-se que o desempenho de ferramentas tecnológicas de apoio à decisão, além de suplantar as limitações mentais inerentes aos seres humanos, permitem a mitigação de riscos, incertezas, heurísticas e vieses por meio de uma modelagem objetiva e estatística em larga escala, resultando em propostas decisórias ponderadas e eficazes.

Entre diversas possibilidades de emprego militar, foram apresentadas as principais capacidades e aplicações, destacando-se os sistemas autônomos, inteligência de dados, guerra eletrônica, resiliência cibernética, simulação de cenários, manutenção preditiva, medicina de combate, além dos sistemas de apoio à decisão.

O estudo das novas tecnologias permitiu identificar que o desempenho e a confiabilidade são características técnicas fundamentais. Considerando que em contextos militares as soluções devem integrar requisitos específicos de tolerância a falhas, segurança e resiliência, assegurando que o sistema não apenas opere rapidamente, mas também de forma confiável, e em consonância com objetivo principal proposto neste trabalho, foram analisados os principais requisitos de confiabilidade para sistemas militares de apoio à decisão, os quais devem orientar desenvolvedores e usuários, sendo eles estudados e definidos como a transparência algorítmica, explicabilidade, interoperabilidade, robustez, redundância e responsabilidade.

Para a transparência algorítmica foi concluído que o modelo de *design* transparente a ser utilizado deve possuir metadados específicos e customizáveis, com a capacidade de registro das interações humanas e, em se tratando de sistemas decisórios, da lógica decisória primária, dos filtros aplicados e da base de dados utilizada. Mesmo que na contramão do conceito básico de transparência, este trabalho orienta a evitar a utilização de códigos abertos por representar um risco de vulnerabilidade para ataques maliciosos ou exploração adversária. A solução proposta é a segmentação da transparência em camadas, protegendo as informações sensíveis que poderiam comprometer a lógica e o pensamento estratégico, enquanto aspectos menos críticos podem ser acessíveis para auditorias e melhorias colaborativas, proporcionando o equilíbrio necessário da segurança com os benefícios da transparência.

O requisito de explicabilidade foi analisado com a mesma lógica de verificação por camadas intermediárias, concluindo com a proposição da adoção de métodos de simplificação de interpretações locais e globais, por meio do uso de *dashboards* de monitoramento em tempo real de indicadores de performance e de governança. Por meio de acompanhamento dinâmico, a explicabilidade assegura que as ações baseadas em IA ou sistemas decisórios autônomos sejam tomadas de forma responsável, permitindo a possibilidade de interações humanas tempestivas e corretivas, de forma a minimizar o risco de desvios comportamentais indesejados decorrentes de erros, vieses algoritmos ou influência maliciosa oponente.

A interoperabilidade sistêmica foi determinada pelo cumprimento de um conjunto de condições organizacionais e técnicas. Concluiu-se que os sistemas de IA que dão suporte ao processo decisório são também dependentes de definições claras e objetivas dos aspectos organizacionais. Foi também concluído que devem ser evitadas iniciativas isoladas de cada FA no desenvolvimento de qualquer sistema que se vislumbre a possibilidade de emprego conjunto, de forma que se evite o risco de falta de padronização de protocolos e de modelagem de dados. Concluiu-se, ainda, que as bases de dados de cada FA devem adotar estruturas que realizem validação cruzada, como forma de verificação e ampliação das capacidades individuais e que não se trata de um *trade-off* entre perda de poder decisório ou autonomia, mas de uma evolução da cultura do processo decisório.

A capacidade de lidar com erros de execução, de entrada de dados errados ou insuficientes, falhas internas ou vulnerabilidades que possam ser exploradas por adversários, evitando-se o risco de uma resposta não executável ou fora dos padrões de conformidade estabelecidos foi tratada como requisito de robustez. Mais uma vez, concluiu-se que a utilização de técnicas de validação cruzada em diferentes subconjuntos de dados de cada FA e do monitoramento de comportamento anômalo podem resultar em eficazes soluções técnicas de minimização do risco. Foram também estudadas as possíveis falhas acidentais ou intencionais decorrentes de programações ocultas em nível de hardware que podem induzir comportamentos de difícil identificação em sistemas de apoio à decisão, concluindo que se trata de um risco que não pode ser evitado a não ser pela produção autóctone, mas que pode ser mitigado por meio de execução de contínuas auditorias de segurança, transparência dos fornecedores e atualizações constantes.

A redundância foi verificada como um requisito determinante para a

salvaguarda do funcionamento confiável sem solução de continuidade dos sistemas de apoio à decisão militar. Novamente a utilização da comparação de entrada de dados entre diferentes fontes e a validação cruzada em camadas segmentadas foram a soluções técnicas propostas. Dessa forma, sistemas de IA podem efetuar correlações comparativas dinâmicas e sem interrupções em níveis inferiores, promovendo possíveis correções antes do processamento decisório final. Em termos físicos, concluiu que sistemas decisórios críticos devem considerar a possibilidade de possuir estruturas paralelas, síncronas e com chaveamento automático, sendo apresentado o modelo do sistema SIGMA operado pela FAB.

A utilização ética, justa e segura por meio do gerenciamento de riscos de discriminação algorítmica, principalmente em sistemas de decisão autônoma, foi estudada no requisito de responsabilidade. Neste sentido, foi concluído que sistemas decisórios militares devem incorporar mecanismos de autoproteção de competências, de decisões anômalas e implementar barreiras múltiplas verificação em função da criticidade da decisão. Durante a análise, foi verificado que questões éticas e jurídicas relacionadas ao emprego de SNT e LAWS carecem de definições bem estabelecidas de forma a convergir para um *design* algoritmo confiável e que a falta de um posicionamento estratégico nacional infere uma incerteza de modo análogo à adesão ao TNP, onde países detentores de tecnologias críticas limitam o desenvolvimento dos demais que não as possuem.

Ao analisar individualmente cada um dos principais requisitos de confiabilidade para sistemas de apoio às decisões militares, também foi possível concluir a existência de profundas relações de interdependência e que são necessárias otimizações conjuntas entre as partes interessadas para mudar o paradigma do *trade-off* entre os requisitos, condição fundamental para o desenvolvimento de novas táticas e a ruptura de paradigmas estratégicos.

Além de evidenciar que o uso de novas ferramentas tecnológicas no processo decisório oferece vantagens diferenciais, com potencial de revolucionar os assuntos militares em termos de eficiência, rapidez e precisão, a identificação e análise dos principais requisitos de confiabilidade resultaram, como principal contribuição do estudo, no desenvolvimento de diretrizes fundamentais para garantir a confiabilidade operacional e a segurança algorítmica em sistemas de apoio à decisão militar. Isso minimiza a influência de heurísticas, vieses cognitivos e fatores emocionais, mitigando riscos e incertezas.

A continuidade deste trabalho é fundamental para garantir que a confiabilidade das novas tecnologias esteja em consonância com os futuros desafios e oportunidades que surgirão com o progresso tecnológico. Essa constante evolução trará à tona novas discussões sobre a relação entre a subjetividade humana e os efeitos emocionais na racionalidade, em contraste com o pragmatismo da lógica algorítmica de sistemas, abrangendo questões técnicas, morais, éticas e normativas.

REFERÊNCIAS

AMARANTE, J. Carlos. **O Voo da Humanidade e 101 Tecnologias que Mudaram a Face da Terra**. Rio de Janeiro: Biblioteca do Exército, 2009.

ASIMOV, Isaac. **Eu, Robô**. 1. ed. São Paulo: Aleph, 2014.

BRASIL. **Lei nº 14.133, de 01 de abril de 2021**. Estabelece normas gerais de licitação e contratação para as Administrações Públicas. Diário Oficial da União: Edição 61-F, Seção 1, Brasília, DF, 1º abr. 2021.

BRASIL. Ministério da Ciência, Tecnologia e Inovação. **Proposta de Plano Brasileiro de Inteligência Artificial**. Brasília, DF, 2024. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2024/07/plano-brasileiro-de-ia-tera-supercomputador-e-investimento-de-r-23-bilhoes-em-quatro-anos/ia_para_o_bem_de_todos.pdf/view. Acesso em: 3 ago. 2024.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa** - Brasília, DF. 2020. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf. Acesso em: 10 mar. 2024.

BRASIL. **Projeto de Lei nº 2.338, de 2023**. Dispõe sobre o uso da Inteligência Artificial. Apresentado em 03 de maio de 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 2 ago. 2024.

BRASIL. Ministério da Defesa. Comando da Aeronáutica. **Gestão de Riscos no Comando da Aeronáutica**. Diretriz do Comando da Aeronáutica 16-2, 2022.

BRASIL. Ministério da Defesa. **Doutrina de Operações Conjuntas – MD30-M-01** Volumes 1 e 2. 2ª Edição, 2020.

CHOLLET, F. ***Deep Learning with Python (First)***. Manning Publications Co. 2018

CLAUSEWITZ, Carl von. **Da Guerra**. São Paulo, SP: WMF Martins Fontes, 2010.

COVELLO, V. T.; MUNPOWER, J. ***Risk analysis and risk management: an historical perspective****. Risk Analysis*, v. 5, n. 2, p. 103-120, 1985.

DARPA – Defense Advanced Research Projects Agency – Special Notice-18-80. **Serial Interactions in Imperfect Information Games Applied to Complex Military Decision-Making**. 2018. Disponível em: https://www.darpa.mil/program/serial-interactions-in-imperfect-information-games-applied-to-complex-military-decision-making. Acesso em: 15 abr. 2024.

ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA (ENAP). **Introdução à Interoperabilidade**. Módulo 1. Brasília, 2015. Disponível em: https://repositorio.enap.gov.br/handle/1/2399. Acesso em: 20 mar. 2024.

ESTADOS UNIDOS. *U.S. Department of Defense*. ***National Defense Strategy 2022***. Washington, DC: Department of Defense, 2022. Disponível em https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF . Acesso em: 17 jun.2024.

FREITAS, C. M. de ; GOMEZ, C. M. **Análise de riscos tecnológicos na perspectiva das ciências sociais**. História, Ciências, Saúde, Manguinhos, v. 3, n. 3, p. 500-504, 1997.

FREITAS, H.M.R. **A Informação com Ferramenta Gerencial**. Porto Alegre: Ortiz, 1993.

FREITAS, H.M.R.; KLADIS, C.M. **O Processo Decisório: modelos e dificuldades**. Rio de Janeiro: Revista Decidir, ano II, n. 08, mar. 1995, p. 30-34 Disponível em https://www2.unifap.br/furtado/files/2017/04/1995_028_rev_decidir.pdf. Acesso em15 abr. 2024.

FULLER, R. Buckminster. ***Critical Path***. New York: St. Martin's Press, 1982.

GROSS, J. C. **Multicritério de apoio à decisão**. Indaial: UNIASSELVI, 2010.

HWANG, Gyusun; HAN, Jun-Hee; CHANG, Tai-Woo. ***An Integrated Key Performance Measurement for Manufacturing Operations Management***. Sustainability, 2020. Disponível em: https://doi.org/10.3390/su12135260. Acesso em: 20 jul. 2024.

KAHNEMAN, Daniel. **Rápido e Devagar: duas formas de pensar**. Rio de Janeiro: Objetiva, 2012

KEYNES, J. M. ***The General Theory of Employment***. The Quarterly Journal of Economics, February. The collected writings of John Maynard Keynes, v. 14, p. 109-123, 1937a.

KNIGHT, F. ***Risk, Uncertainty and Profit***. London: Houghton Mifflin, 1921.

KRENKER, Andrej; BEŠTER, Janez; KOS, Andrej. ***Introduction to the Artificial Neural Networks***. Em: SUZUKI, Kenji (editor). *Artificial Neural Networks - Methodological Advances and Biomedical Applications*. InTech; 2011. Disponível em: http://dx.doi.org/10.5772/644. Acesso em: 25 jun. 2024.

KURZWEIL, Ray. ***The Singularity is Near: when humans transcend biology***. New York: Viking, 2005.

LEVIN, J. ***Choice under uncertainty***. Stanford University. 2006.

LI, Bo; LIU, Bo; DI, Shuai; LIU, Jingen; PEI, Jiquan; YI, Jinfeng; ZHOU, Bowen. ***Trustworthy AI: From Principles to Practices***. ACM Computing Surveys, Vol. 55, No. 9, Article 177. New York, United States: Association for Computing Machinery, 2023. Disponível em: https://dl.acm.org/doi/pdf/10.1145/3555803. Acesso em: 18 mar. 2024.

LUGER, George F. **Inteligência Artificial**. 6ª. ed. São Paulo: Pearson, 2013

McCARTHY, John. ***What is Artificial Intelligence?*** Stanford: Stanford University, 2007. Disponível em: http://jmc.stanford.edu/articles/whatisai/whatisai.pdf. Acesso em: 30 mar. 2024

MOORE, Gordon E. ***Cramming More Components onto Integrated Circuits***. Electronics, v. 38, n. 8, 19 abr. 1965.

MOUBRAY, J. ***Reliability Centered Maintenance***. New York, Editora Industrial Press, Revisão da 2ª Edição, 2001.

NAVARRO, Marcus V.T. **Conceito e controle de riscos à saúde**. Em: Risco, Radiodiagnóstico e Vigilância Sanitária. Salvador: EDUFBA, 2009, pp. 37-75. Disponível em: http://books.scielo.org. Acesso em: 23 maio 2024.

OECD. ***Revised Recommendation of Council on Artificial Intelligence***. Meeting of the Council at Ministerial Level, 2-3 May 2024. Disponível em: https://one.oecd.org/document/C/MIN(2024)16/FINAL/en/pdf. Acesso em: 01 ago. 2024.

PICCININI, Gualtiero. ***The First Computational Theory of Mind and Brain: A Close Look at Mcculloch and Pitts Logical Calculus of Ideas Immanent in Nervous Activity***. Netherlands: Synthese, 2004.

SAATY, T.L. ***How to make a decision: The analytic hierarchy process***. European Journal of Operational Research, Amsterdam, v.48, p.9-26, 1990.

SCHILLING, D. Russel. ***Knowledge Doubling every 12 month, Soon Doubling every 12 hours***. Industry Tap into News, 2013. Disponível em: https://www.industrytap.com/knowledge-doubling-every-12-months-soon-to-be-every-12-hours/3950. Acesso em: 10 jul. 2024.

SCHOEMAKER, Paul J. H. ***The Expected Utility Model: Its Variants, Purposes, Evidence and Limitations***. Journal of Economic Literature, v. 20, n. 2, p. 529-563, 1982.

SHALEV-SHAWARTZ, Shai, BEN-DAVI, Shai. ***Understanding Machine Learning: From Theory to Algorithms*.** Cambridge University Press, 2014. Disponível em: https://www.cs.huji.ac.il/~shais/UnderstandingMachineLearning/understanding-machine-learning-theory-algorithms.pdf. Acesso em: 12 jul. 2024.

SIMON, Herbert. A. ***Administrative Behavior: a Study of Decision-Making Processes in Administrative Organization***. 3a. Edição. Nova York: Free Press, 1976.

SOMMERVILLE, I. **Engenharia de Software**. 9ª Ed; Pearson Addison. Wesley. São Paulo, 2011.

SRINIVASARAGHAVAN, Anuradha; JOSEPH, Vincy. ***Machine Learning***. New Delhi: Wiley, 2020.

TOTVS. ***Data driven*****: o que é gestão de negócios baseado em dados e como aplicar** . Disponível em: https://www.totvs.com/blog/inteligencia-de-dados/data-driven/. Acesso em: 28 maio 2024.

VON NEUMANN, John; MORGENSTERN, Oskar. ***Theory of Games and Economic Behavior***. 3. ed. Princeton: Princeton University Press, 1953.

YÜKSEL, İ.; DAĞDEVIREN, M. ***Using the analytic network process (ANP) in a SWOT analysis – A case study for a textile firm***. Information Sciences, Vol. 177, No. 16, pp. 3364-3382, 2007

TOLK, Andreas. ***Beyond Technical Interoperability: Introducing a Reference Model for Measures of Merit for Coalition Interoperability***. In: International Command and Patrol Research and Technology Symposium, 2003, Washington D.C. Disponível em: https://apps.dtic.mil/sti/pdfs/ADA466775.pdf. Acesso em: 19 jul. 2024.

TONIN, Matej - ***Artificial Intelligence: implications for NATO's Armed Forces***. 65th *NATO Parliamentary Assembly*. Londres, 2019. Disponível em: https://www.nato-pa.int/download-file?filename=/sites/default/files/2019-10/REPORT%20149%20STCTTS%2019%20E%20rev.%201%20fin-%20ARTIFICIAL%20INTELLIGENCE.pdf. Acesso em: 15 jun. 2024.

TURING, Alan M. ***Computing Machinery and Intelligence***. Mind, New Series, Vol. 59, Nº. 236 (1950). Disponível em: http://www.jstor.org/stable/2251299. Acesso em: 26 jun. 2024.

WILLIAMS, Blair S. **Heurísticas e Vieses no Processo Decisório Militar**. Military Review, Army University Press, jan-fev 2011. Disponível em: https://www.armyupress.army.mil/journals/edicao-brasileira/artigos-em-destaque/2018/heuristicas-e-vieses-no-processo-decisorio-militar/. Acesso em: 28 mar. 2024.

APÊNDICE A – Capacidades e Aplicações de novas tecnologias em ambientes militares

Capacidades	Aplicações
Sistemas Militares Autônomos	Veículos ou dispositivos equipados com sistemas que aprendem e tomam decisões sozinhos, que podem ser utilizados em missões de vigilância, reconhecimento, ataque, apoio logístico e desminagem em zonas de conflito, com maior precisão e sem a necessidade de exposição ao perigo de um operador humano.
Inteligência, Síntese e Análise de Dados	Ferramentas que podem processar grandes volumes de textos, imagens ou vídeos de fontes diversas, fornecendo informações de inteligência e de monitoramento do campo de batalha em tempo real.
Guerra Eletrônica	Realizar a interceptação, quebra da criptografia, decodificação e análise das comunicações inimigas no campo de batalha. Em outra abordagem, podem ser utilizados para realizar ataques eletrônicos, como bloqueio das comunicações inimigas ou interferência em seus sistemas de radar.
Aumento da Segurança e da Resiliência Cibernética	Identificação de atividades anômalas relacionadas à espionagem ou tentativas de ataque cibernético em redes militares, reagindo rapidamente de forma bloquear acessos indevidos, mitigar danos e manter a continuidade das operações.
Auxílio à Tomada de Decisão	Considerando a extensa base de dados e atualização em tempo real, sistemas de apoio à decisão baseados em novas tecnologias podem sugerir cursos de ação e apresentar análises estatísticas em tempo real por meio de assistentes virtuais em linguagem natural, ferramentas que podem auxiliar os Comandantes na tomada de decisões sejam táticas, operacionais ou estratégicas.
Simulação	Criação de cenários dinâmicos em realidade virtual ou aumentada, podendo ser empregados em treinamento de combatentes ou na previsão de resultados de diferentes estratégias.
Manutenção Preditiva	A integração de equipamentos que realizam e informam suas condições por autodiagnóstico com sistemas de manutenção inteligente estenderão a vida útil e evitarão falhas nos equipamentos, reduzindo custos e o tempo de inatividade, além de aumentar a segurança operacional.
Medicina em Combate	Sensores implantados em combatentes e conectados a sistemas assistidos sistemas inteligentes podem monitorar as suas funções vitais, permitindo diagnósticos antecipados e otimizações nos atendimentos médicos em zonas de conflito.