Estudo do emprego de Inteligência Artificial no contexto da Guerra Cibernética

Capitão-Tenente Françoa Taffarel Rosário Corrêa*

RESUMO

Os avanços contínuos no setor de Tecnologia da Informação e Comunicação implicam no surgimento de novos desafios para a Guerra Cibernética (GCiber). Este artigo se concentra na aplicação de Inteligência Artificial (IA) em operações ofensivas de GCiber. Através de uma revisão bibliográfica, foi apresentado e analisado o contexto geopolítico do desenvolvimento de IA em países como China, Estados Unidos, Índia e Rússia. Como resultado desta pesquisa vislumbramos a apresentação de possíveis cenários de ataques cibernéticos baseados em IA. Por fim, foi possível identificar indícios de uma nova postura do Brasil no desenvolvimento da IA, bem como foram elencadas recomendações para garantir o contínuo progresso do governo brasileiro na utilização da IA.

Palavras-chave: Inteligência Artificial; Guerra Cibernética; Aplicação.

Study of usage of Artificial Intelligence in the context of Cyber Warfare

ABSTRACT

Continuous advances in the Information and Communication Technology sector imply the emergence of new challenges for Cyber Warfare. This article focuses on the application of Artificial Intelligence (AI) in Cyber Warfare offensive operations. Through a literature review, the geopolitical context of the development of artificial intelligence in countries like China, the United States, India and Russia was presented and analyzed. As a result of this research, we envision the presentation of possible scenarios of cyber attacks based on AI. Finally, it was possible to identify evidence of a new posture by Brazil in the development of AI, as well as recommendations to guarantee the continuous progress of the Brazilian government in the use of AI.

Keywords*: Artificial Intelligence; Cyber War; Application*.

1 INTRODUÇÃO

O desenvolvimento das Tecnologias da Informação e Comunicações (TIC) permitiu a expansão da internet, que de forma proporcional introduziu inúmeras inovações aos seus usuários (PEREIRA, 2018). Entretanto, essas inovações estão acompanhadas de ameaças no ambiente cibernético[1] as quais são mais inteligentes, sofisticadas e complexas elevando de forma exponencial os desafios de segurança e os riscos associados durante a utilização de dispositivos computacionais. Segundo Handa (2020), essa exponencialidade tem como uma de suas justificativas o uso de Inteligência Artificial (IA) em ações de Guerra Cibernética[2](GCiber[3]) a fim de garantir que haja adaptabilidade frente a mecanismos de defesa permitindo uma tomada de decisão em cada situação de ataque.

De acordo com Tyugu (2007), a IA pode ser idealizada de duas maneiras: como uma ciência destinada a tentar descobrir a essência da inteligência e desenvolver máquinas inteligentes, ou como uma ciência que fornece métodos para resolver problemas complexos que não podem ser resolvidos por técnicas ou ferramentas convencionais a fim de elevar a rapidez na correta tomada de decisão com base em grandes quantidades de dados.

A presente pesquisa adotou a segunda visão com o objetivo de evidenciar a aplicação da IA com ênfase em operações de GCiber. Justifica-se esta pesquisa devido ao fato que a IA é um potencializador do domínio cibernético frente a sua alta capacidade de aprendizado e aplicação de conhecimento tornando-se um diferencial na GCiber.

[1] Ameaça no ambiente cibernético é o conjunto de fatores externos de um incidente indesejado, que pode resultar em dano para uma organização através de ativos relacionados ao meio cibernético como dispositivos e sistemas conectados em rede. (BRASIL, 2019).

[2] A guerra cibernética é o conjunto de atos de guerra que utilizam prioritariamente elementos de TIC, por um período específico de tempo e em alta velocidade, em apoio a operações militares através de ações tomadas exclusivamente no espaço cibernético. (BRASIL, 2019).

[3] Este estudo adotou o padrão de abreviaturas previsto no Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas – MD33-M-02. (BRASIL, 2008).

De forma a fundamentar e gerar consistência teórica, foi conduzida uma pesquisa bibliográfica qualitativa em obras elaboradas por autores da Iniciativa de Inteligência Cibernética do Instituto de Política Mundial e do Centro de Excelência em Defesa Cibernética Cooperativa da Organização do Tratado do Atlântico Norte.

Na seção 2, será exposta uma caracterização da IA no âmbito da GCiber, bem como a atual estrutura geopolítica sobre essa questão. Em seguida, na seção 3, serão apresentados possíveis cenários de ataques cibernéticos baseados em IA. Por fim, serão enumeradas conclusões desta pesquisa e as sugestões para trabalhos futuros.

2 A INTELIGÊNCIA ARTIFICIAL NO ÂMBITO CIBERNÉTICO

Segundo Tyugu (2007), a IA nasceu como uma disciplina de pesquisa na universidade americana *Dartmouth College* em 1956, como um subcampo da ciência da computação que executa habilidades cognitivas através do aprendizado em sistemas de computador. Neste mesmo contexto, para Allen e Chan (2018), a IA tem a capacidade de desenvolver habilidades abrangentes de resolução de problemas em seus próprios algoritmos, o que a faz crescer de forma exponencial.

Além disso, conforme entendimento de Tyugu (2007) a IA aplica análises avançadas e técnicas baseadas em lógica, para interpretar eventos, apoiar e automatizar decisões e realizar ações através dos algoritmos de *Machine Learning* (ML) que segundo Ethem Alpaydin são definidos como:

> [...] a programação de computadores para otimizar um critério de desempenho usando dados de exemplo ou experiências anteriores. Existindo um modelo definido até alguns parâmetros, o aprendizado é a execução de um programa de computador para otimizar os parâmetros do modelo usando os dados de treinamento ou experiência anterior. O modelo pode ser preditivo para fazer previsões no futuro ou descritivo para obter conhecimento dos dados, ou ambos. (ALPAYDIN, 2020, p. 3, tradução nossa).

Conforme exposto no Relatório Anual de Predições sobre IA (PWC, 2020), aprimorar a segurança cibernética está se tornando cada vez mais desafiador, devido ao número crescente de dispositivos conectados à internet e de volume de dados produzidos que precisam de proteção. Segundo esse relatório, o volume é tal que os humanos nunca serão capazes de monitorar redes de dados sem a assistência de máquinas. Assim, o potencial da IA nesta área é evidenciado especialmente no aumento da capacidade dos operadores humanos de monitorar e responder a eventos adversos e anormais.

Contudo, conforme elencado por Meinert (2018), além do paradigma da utilização da IA como defesa no espaço cibernético, salienta-se ainda que os especialistas em cibersegurança e chefes de comandos militares especializados em GCiber poderão elevar a eficácia de suas equipes ofensivas durante ataques cibernéticos em um cenário de utilização de ferramentas baseadas em IA.

Assim, uma equipe de ação ofensiva ao utilizar técnicas de GCiber baseadas em IA pode oferecer vantagens estratégicas aos atacantes, por meio da capacidade autônoma da IA em interromper e destruir sistemas inimigos através de operações cibernéticas.

Segundo Browne (2018), uma ação tática ofensiva pode incluir o aproveitamento da IA para transformar dispositivos computacionais em armas potenciais, pois diversas infraestruturas críticas como centrais nucleares ao serem desestabilizadas podem causar danos tanto ao meio ambiente quanto danos físicos aos humanos. Vale salientar ainda que a IA também pode trazer grandes avanços tecnológicos para a guerra convencional, incluindo a implementação de sistemas de armas que podem ter recursos totalmente autônomos e capazes de solucionar problemas complexos.

Além disso, segundo Vasudevan (2018), os sistemas atuais geram tantos dados de segurança que os especialistas humanos são rapidamente ultrapassados, garantindo assim uma posição vantajosa em um efetivo ataque cibernético a atores específicos.

2.1 A GEOPOLÍTICA DA APLICAÇÃO DA INTELIGÊNCIA ARTIFICIAL EM GUERRA CIBERNÉTICA

De acordo com Simonite (2018) os Estados Unidos da América (EUA) são apenas um dos muitos investidores em IA, seguidos pela China e por muitas outras nações estão tomando medidas para garantir sua competitividade nesse setor. Segundo Metz (2018), atualmente os EUA, através do Departamento de Defesa dos Estados Unidos, atua de forma sistemática com a integração da IA em todos os escalões da estrutura organizacional.

Conforme Boyd (2018), o Departamento de Defesa determinou que a IA fosse tratada como prioridade principal na pesquisa e desenvolvimento, e anunciou planos para estudar métodos de como garantir que os EUA continuem sendo líderes mundiais em IA. Parte desses planos incluíam a construção de uma base de recursos humanos responsáveis pelo desenvolvimento de tecnologia baseada em IA, bem como uma maior aproximação da indústria privada, a fim de elevar uso da IA nas forças armadas em operações de GCiber.

Segundo Kai-Fu (2018), a supremacia dos EUA como líder global em IA, está enfrentando desafios, pois cada vez mais, as nações em todo o mundo estão mobilizando apoio político para avanços em tecnologias e aplicações baseadas em IA reconhecendo sua importância para economia e para elevação de suas capacidades militares. O mesmo autor prevê o surgimento de um duopólio entre os EUA e a China como superpotências em IA, seguidos pela Índia e Rússia.

Assim, em relação a China, é valido ressaltar que através do Plano de Desenvolvimento de Inteligência Artificial da Nova Geração (CHINA, 2017) emitido pelo seu Conselho Estatal, este país iniciou sua ascensão no processo de potência em IA. Este plano prevê o desenvolvimento de uma indústria tecnológica em IA através da aplicação financeira de cerca de 150 bilhões de dólares até 2030 com o propósito de garantir uma posição estratégica no âmbito do domínio da IA.

Segundo Triolo e Kania (2018), a fim de realizar o desenvolvimento da indústria de IA, o governo chinês está alavancando o dinamismo das empresas comerciais privadas com setores públicos, criando uma fusão civil-militar como forma de estratégia para alcançar os avanços previstos no plano citado anteriormente e estabelecer vantagem competitiva internacional.

No contexto GCiber, à medida que a China oferece apoio e recursos do Estado à indústria para o desenvolvimento da IA, as principais empresas de tecnologia chinesas têm se tornado contínuos participantes nesse esforço. Atualmente, de acordo com Jia *et al.* (2017), a empresa de Tecnologia Baidu através do Laboratório Nacional de Engenharia Chinês é responsável pela construção de ferramentas ofensivas baseadas em IA que serão utilizadas na GCiber em operações ofensivas do Exército de Libertação Popular.

Conforme Bhatia (2018), em relação a Índia, cabe salientar que o governo indiano está começando a explorar medidas políticas que possam permitir o surgimento de um ecossistema de IA robusto que atuará na próxima década, em diversos setores como saúde, educação e infraestrutura críticas, bem como no setor militar.

Segundo Menon e Vazirani (2017), o governo indiano está trabalhando para criar programas profissionais que permitem aos alunos obter certificações em IA. Em contrapartida, de acordo com Vempati (2018), atualmente a Índia carece de especialização adequada, especialmente em relação aos EUA e à China. Ressalta-se ainda, que Vempati ainda elenca que diversas faculdades de engenharia na Índia não têm currículos adequados para produzir um fluxo robusto de talentos especialistas em IA, o que impactaria no desenvolvimento de artefatos maliciosos para operações em GCiber.

Nesse contexto, uma dessas medidas foi a publicação da Estratégia Nacional de Inteligência Artificial (INDIA, 2018) que por intermédio do Departamento de Produção de Defesa da Índia estabeleceu a Força-Tarefa para estudar aplicações da IA no âmbito militar, com o propósito de fomentar o desenvolvimento de artefatos baseados em IA para operações de GCiber.

Corroborando com essa atitude, segundo Rafiq (2019), a ativação da Agência de Defesa Cibernética Indiana (ADC) em 2019 foi fundamental para definir os atores do governo indiano, os quais serão responsáveis por ações ofensivas de GCiber que utilizarão aplicações baseadas em IA criadas na Organização de Pesquisa e Desenvolvimento de Defesa da Índia e no Centro de Inteligência Artificial e Robótica.

No que se refere a Rússia, de acordo com Bendett (2018), embora esse Estado possa não ter o dinamismo gerador de inovação em IA dos EUA e da China, existem grandes esforços da indústria de defesa russa para fazer avançar as aplicações militares baseadas em IA permitindo sua utilização em operações de GCiber. Bendett ainda afirma que os níveis atuais de investimento na Rússia, estimados em 12,5 milhões de dólares, são bastante baixos em relação aos gastos governamentais dos EUA e da China.

Nesse contexto, conforme Bendett (2018), enquanto o desenvolvimento da IA nos EUA e na China avançou por meio de empresas comerciais dinâmicas, na Rússia o Ministério da Defesa, através do órgão público chamado Fundação para Estudos Avançados da Rússia, tem iniciado novos projetos envolvendo sistemas de IA que serão utilizados pelo Ministério da Defesa russo em operações cibernéticas.

Frente ao exposto acima, impende ressaltar que há um risco crescente para a liderança militar global dos EUA, dada a amplitude da IA, com sua capacidade de influenciar a defesa, a competitividade econômica e o desenvolvimento de ferramentas para GCiber.

3 CENÁRIOS DE UTILIZAÇÃO DA IA NA GUERRA CIBERNÉTICA

Segundo Morgan *et al.* (2009), com a GCiber como uma preocupação militar atual e crescente, a qual se origina no mesmo ambiente da IA espera-se que existam interseções entre as mesmas.

Esses pontos em comum foram corroborados pelo Relatório de Previsões de Segurança Cibernética da Symantec (SYMANTEC, 2018), que evidenciou um aumento das ações de invasores cibernéticos utilizando técnicas de IA. Conforme Brundage *et al.* (2018) cresce de importância que os especialistas em cibersegurança entendam como será o cenário da GCiber no futuro por meio da utilização da IA.

Segundo Whyte (2020), a resposta essa pergunta é que a IA tornará os ataques cibernéticos mais poderosos, reduzindo a eficácia das medidas defensivas convencionais. Whyte ainda afirma que os artefatos maliciosos utilizados nos cenários das operações de GCiber baseados em IA, são influenciados por quatro características. São elas:

a) O aumento da superfície de ataque em escala e velocidade:
- caracterizado pela oportunidade dos artefatos de ataque utilizarem os dados de entrada obtidos por meio da infecção de máquinas para julgar probabilisticamente onde e quando outro ataque pode ser relevante;

b) Adaptação Técnica:
- é a capacidade do artefato baseado em IA, de selecionar autonomamente formas de exploração dentro de servidores alvo;

c) Adaptação Tática Adversarial:
- caracterizado por um artefato possuir condições de ajustar sua própria estratégia de abordagem conforme as ações contra sistema alvo; e

d) Múltiplas mentalidades:
- é a capacidade que o artefato possui de analisar as redes do sistema alvo e agir de forma autônoma para atacar ou não, a fim de maximizar as oportunidades futuras.

Serão enumerados nas próximas subseções aplicações da IA com fins ofensivos no contexto da GCiber.

3.1 ATAQUES DE PHISHING UTILIZANDO A IA

Conforme Finnie (2018), ataques automatizados pela IA *phishing*[4] podem ocorrer através da adulteração do filtro de spam de forma que não seja possível identificar que as mensagens são maliciosas.

Segundo a Cyxtera Technologies (2018) em um contexto prático atualmente existem dois trabalhos relevantes que utilizam algoritmos de ML como uma ferramenta para ataques de phishing. São eles:

a) Honey-Phish:
- o projeto Honey-Phish, possui em seu banco de dados diversas coleções de e-mails anteriormente caracterizados como phishing e através de algoritmos de ML automatiza as respostas aos *e-mails* de *phishing* para estabelecer uma comunicação por e-mail com o alvo permitindo assim que *e-mails* falsos sejam considerados reais; e

b) Deep Domain Generation Algorithms (DGA)[5]:
- a abordagem *Deep* DGA usa Redes Adversárias Generativas[6] para criar domínios artificiais de difícil detecção por filtros dos provedores de e-mails.

3.2 ARTEFATOS MALICIOSOS BASEADOS EM IA

De acordo com Finnie (2018), a IA poderá ser usada para aprimorar um *malware*, permitindo que ele seja autossuficiente no aprendizado do ambiente em que se encontra, a fim de que ele possa passar desapercebido por antivírus e sistema de defesa de rede.

Assim, o *malware* poderá evitar detecções permitindo a sua operação sobre os dados do sistema alvo. De uma perspectiva ofensiva, a IA poderá aproveitar a grande gama de dispositivos disponíveis na rede para elevar a velocidade e adaptabilidade de um ataque por meio de algoritmos de ML.

Segundo Kubovič (2018), os sistemas de ataque aprenderão como e quando atacar o sistema alvo, sendo capazes de mudar o comportamento quando sob contra-ataque e de buscar novas vulnerabilidades no momento em que vetor de ataque original é mitigado por um software de detecção.

Dessa forma, artefatos que utilizarão a IA como forma de aprender sobre o ambiente defensivo do sistema alvo, bem como adotar medidas alternativas podem conduzir a atividade onde os parâmetros da missão são considerados alterados.

3.3 ATAQUES CIBERNÉTICOS MULTIVETORIZADOS

O estudo de Inteligência Artificial (IA) em Segurança Cibernética do Ponemon Institute de 2018 (PONEMON, 2018) indica que a IA é capaz de detectar 63 por cento de novas vulnerabilidades.

[4] Phishing é o tipo de fraude na qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização de engenharia social e técnicas digitais. (CERT, 2020).

[5] Algoritmos de geração de domínio (DGA) são algoritmos usados para gerar um grande número de nomes de domínio de rede, utilizados em ações de Phishing. (ANDERSON, 2018).

[6] Redes Adversárias Generativas (GANs) são arquiteturas de redes neurais profundas compostas por duas redes colocadas uma contra a outra. (ANDERSON, 2018).

Com isso, é valido salientar que a IA diminuirá a quantidade de humanos na condução de ataques cibernéticos, com máquinas automatizadas capazes de reunir informações através de Fuzzing[7]. Assim, a IA reunirá informações suficientes para iniciar ataques cibernéticos de larga escala. É importante destacar que ataques baseados em IA poderão ter suas táticas alteradas de acordo com os parâmetros da missão à medida que aprende mais sobre o ambiente do sistema alvo.

Segundo Comiter (2019), os cenários de ataques multivetorizados baseados em IA buscam depreender as operações do sistema e rotinas de defesa do sistema alvo. Comiter também afirma que esses ataques podem se enquadrar em duas categorias. São elas:

a) Ataques de entrada:
- ataques de entrada os quais buscam fundamentalmente enganar um sistema de IA e distorcer os esforços desse sistema para classificar padrões de atividade; e

b) Ataques de envenenamento:
- os ataques de envenenamento são atividades que buscam fundamentalmente comprometer o sistema alvo através da manipulação de dado padronizados de forma a corromper o contínuo funcionamento ocasionando instabilidade ou total negação de usabilidade do sistema.

4 CONSIDERAÇÕES FINAIS

Pela coadunação do exposto nas sessões anteriores, impende afirmar que o contínuo avanço tecnológico da IA no âmbito da GCiber permite uma posição estratégica relevante para qualquer país que inicia e fomenta continuamente o setor. Dessa forma, este trabalho expôs como ferramentas baseadas em IA podem ser aplicadas em operações ofensivas de GCiber, bem como elencou o atual cenário geopolítico dos países que desenvolvem tecnologias relacionadas à IA.

Conforme constatado na revisão bibliográfica exposta e elencado por Kai-Fu (2018), a liderança por outros países não ocorre apenas frente ao domínio da IA em si, mas sobre como ocorre o gerenciamento e aplicação dessas tecnologias baseadas em IA, as quais ao serem utilizadas em operações cibernéticas, inegavelmente oferecerão vantagens estratégicas na diplomacia dos países que as detém.

Nesse contexto, o Brasil está realizando ações para iniciar o desenvolvimento de um ecossistema base para IA, através da criação de diversos centros de pesquisas como o Laboratório de Computação de Alto Desempenho para a Defesa Cibernética (LCAD2C), localizado no Instituto Militar de Engenharia. Soma-se ainda, como passo mais recente, a criação do Centro de Inteligência Artificial (C4AI)[8], laboratório dedicado a estudos e pesquisas sobre IA, localizado no Centro de Pesquisa e Inovação da Universidade de São Paulo. É valido salientar também, que está em tramitação no Congresso Nacional o Projeto de Lei n° 5051 de 2019[9] , o qual estabelece os princípios e regulamentações para o uso da IA.

Contudo, como forma de adotar um modelo para desenvolvimento consolidado da IA no país, constatou-se a necessidade do Brasil realizar, em parceria com o setor privado, uma ampla série de ações, preparando-se para os grandes desafios advindos dos avanços da IA. Estas ações estão relacionadas a:

a) Estratégia:
- para gerenciar os desafios futuros, o Brasil precisa de um Plano Nacional de Inteligência Artificial (PNIA) para aproveitar os benefícios da IA e, ao mesmo tempo, mitigar seus efeitos disruptivos;

b) Pesquisa e Desenvolvimento (P&D):
- o Brasil deve fundamentar o PNIA em P&D, estabelecendo métricas e processos para execução eficaz e desenvolvendo um plano de P&D em IA; e

c) Segurança:
- o governo brasileiro deve aumentar seu investimento em IA em cooperação com a indústria de defesa, a fim de aprimorar as forças armadas com capacidades de executar ações ofensivas cibernéticas com ferramentas baseadas em IA.

Como trabalho futuro, a intenção é realizar uma pesquisa da utilização de ferramentas baseadas em IA em operações de GCiber realizadas pela Marinha do Brasil, bem como outra proposta relevante é realizar uma análise quantitativa das aplicações baseadas em IA em operações ofensivas de GCiber, no que tange sua eficiência e eficácia contra os sistemas de comando e controle e de infraestruturas críticas.

[7] Fuzzing é um método de inserção de dados aleatórios em um sistema alvo, com o propósito de que encontrar possíveis falhas em software ou aplicações web. (TAKANEN, 2018).

[8] O Centro de Inteligência Artificial (C4AI) tem o compromisso de desenvolver pesquisas no estado da arte em Inteligência Artificial (IA). (C4AI, 2020).

[9] O Projeto de Lei (PL) 5.051/2019, aborda o desenvolvimento inclusivo e sustentável da Inteligência Artificial, estabelecendo os princípios para o uso da IA no Brasil, com a finalidade de melhorar o bem-estar humano em geral. (SENADO, 2020).

REFERÊNCIAS BIBLIOGRÁFICAS

ALLEN, G.; CHAN, T. **Artificial Intelligence and National Security**. Washington, DC: Congressional Research Service, 2018. Disponível em: https://thebulletin.org/2018/02/artificial-intelligence-and-national-security/. Acesso em: 25 ago. 2020.

ALPAYDIN, E. **Introduction to Machine Learning**. 2nd. ed. Cambridge: The MIT Press, 2010. E-book.

ANDERSON, H. **Deepdga**: adversarially-tuned domain generation and detection. New York: ACM, 2016. Disponível em: https://www.defenseone.com/ideas/2018/04/russia-races-forward-ai-development/147178/. Acesso em: 10 out. 2020.

BENDETT, S. **In AI, Russia Is Hustling to Catch Up**. Washington, DC: Defense One, Apr. 2018. Disponível em: https://www.defenseone.com/ideas/2018/04/russia-races-forward-ai-development/147178/. Acesso em: 10 out. 2020.

BHATIA, R. **Can India's AI Talent Gap Be Stemmed With Government Initiatives?**. Bengaluru: Analytics India, Feb. 2018. Disponível em: https://analyticsindiamag.com/can-indias-ai-talent-gap-stemmed-government-initiatives/. Acesso em: 09 out. 2020.

BOYD, A. **White House Announces Select Committee of Federal AI Experts**. Washington: Nextgov, 2018. Disponível em: https://bit.ly/3jHtTBX. Acesso em: 07 out 2020.

BRASIL. **Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas**. Brasília, Distrito Federal: Ministério da Defesa, 2008. Disponível em: https://bit.ly/3oJqoyI. Acesso em: 20 ago. 2020.

BRASIL. **Portaria nº 93.** Dispõe sobre Glossário de Segurança da Informação. Brasília, Distrito Federal: Gabinete de Segurança Institucional da Presidência da República, set. 2019. Disponível em: http://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663. Acesso em: 20 set. 2020.

BROWNE, R. **Weaponized drones:** machines that attack on their own. New Jersey: CNBC, July 2018. Disponível em: https://www.cnbc.com/2018/07/20/ai-cyberattacks-artificial-intelligence-threatens-cybersecurity.html. Acesso em: 12 out. 2020.

BRUNDAGE, M.; Avin, S.; Clark, J. et al. **The Malicious Use of Artificial Intelligence**: forecasting, prevention, and mitigation. Disponível em: https://doi.org/10.17863/CAM.22520. Acesso em: 11 out. 2020.

C4AI. **Sobre o C4AI**. São Paulo: C4AI - Centro de Inteligência Artificial, 2020 Disponível em: http://c4ai.inova.usp.br/pt/sobre/. Acesso em: 25 out. 2020.

CERT. **Cartilha de Segurança para Internet**. São Paulo: Comitê Gestor da Internet no Brasil, 2019. Disponível em: https://cartilha.cert.br/livro/cartilha-segurancainternet.pdf. Acesso em: 26 out. 2019.

CHINA. **New Generation of Artificial Intelligence Development Plan**. State Council, 2017. Disponível em: https://flia.org/wp-content/uploads/2017/07/A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf Acesso em: 08 out. 2020.

COMITER, M. **Attacking Artificial Intelligence**: AI's security vulnerability and What Policymakers Can Do About It. Cambridge: Belfer Center for Science and International Affairs, Aug. 2019. Disponível em: https://www.belfercenter.org/publication/AttackingAI. Acesso em: 20 out. 2020.

CYXTERA, T. **DeepPhish:** simulating malicious AI. Flórida: Cyber Threat Analytics, 2018. Disponível em: https://albahnsen.files.wordpress.com/2018/05/deepphish-simulating-malicious-ai_submitted.pdf Acesso em: 08 out. 2020.

FINNIE, S. **Cyber threats fuelled by AI**: security's next big challenge. Framingham: CSO, Oct. 2018. Disponível em: https://bit.ly/34K3qj1. Acesso em: 15 out. 2020.

HANDA, U. **How AI is making organizations more resilient to cybercrime**. London: PWC, Aug. 2020. Disponível em: https://www.digitalpulse.pwc.com.au/ai-cybersecurity-resilience/. Acesso em: 20 ago. 2020.

INDIA. **National Strategy for Artificial Intelligence**. Mumbai: June, 2018. Disponível em: http://www.niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf. Acesso em: 10 out. 2020.

JIA, K.; KENNEY, M.; MATTILA, J. *et al*. **The Application of Artificial Intelligence at Chinese Digital Platform Giants**: Baidu, Alibaba and Tencent. Berkeley: Berkeley Roundtable On The International Economy, Nov. 2018. Disponível em: https://bit.ly/35Pd2sg. Acesso em: 08 out. 2020.

KAI-FU, L. **AI Superpowers**: China, Silicon Valley, and the New World Order. Boston: Houghton Mifflin Harcourt, 2018. E-book.

KUBOVIČ, O. **Can Artificial Intelligence Power Future Malware?**. San diego: ESET White Paper, 2018. Disponível em: https://www.welivesecurity.com/wp-content/uploads/2018/08/Can_AI_Power_Future_Malware.pdf. Acesso em: 11 out. 2020.

MEINERT, M. C. **Artificial Intelligence**: the next frontier of cyber warfare?. Washington, DC: American Bankers Association Banking Journal, 2018. Disponível em: https://www.semanticscholar.org/paper/Artificial-Intelligence%3A-The-Next-Frontier-of-Cyber-Meinert/. Acesso em: 9 out. 2020.

MENON, R. M.; VAZIRANI, M. **Rewire for Growth**: accelerating India's economic growth with Artificial Intelligence. Dublin: Accenture, Dec. 2017. Disponível em: https://www.accenture.com/t20171220T030619Z__w__/in-en/_acnmedia/PDF-68/Accenture-ReWire-For-Growth-POV-19-12-Final.pdf. Acesso em: 9 out. 2020.

METZ, C. **As China Marches Foward on A.I**: the White House is silent. New York: The New York Times, Feb. 2018. Disponível em: https://www.nytimes.com/2018/02/12/technology/china-trump-artificial-intelligence.html. Acesso em: 9 out. 2020.

MORGAN, F.; BOUDREAUX, B.; LOHN, A. *et al*. **Military Applications of Artificial Intelligence**: ethical concerns in an uncertain world. Santa Monica: RAND Corporation, 2020. Disponível em: https://www.rand.org/pubs/research_reports/RR3139-1.html. Acesso em: 12 out. 2020.

PEREIRA, M. **Representação Semântica de Perfil Dinâmico de Usuários em Comunidades de Prática**. Dissertação (Mestrado em Computação) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2018. Disponível em: https://www.lume.ufrgs.br/bitstream/handle/10183/177588/001065807.pdf. Acesso em: 12 out. 2020.

PONEMON, I. **The Value of Artificial Intelligence in Cybersecurity**. Traverse City: Ponemon Institute, July 2018. Disponível em: https://public.dhe.ibm. com/common/ssi/ecm/41/en/41017541usen/ibm-ai-report-final-1_41017541USEN.pdf. Acesso em: 15 out. 2020.

PWC. **Annual Review Predictions AI 2020**. London: PWC, Aug. 2020. Disponível em: https://www.pwc.com/us/en/services/consulting/library/artificial-intelligence-predictions-2020.html Acesso em: 25 ago. 2020.

RAFIQ, A. **Indian cyber posture**: implications for Pakistan. Islamabad: Institute of Strategic Studies, 2019. Disponível em: https://bit.ly/3edVKZv. Acesso em: 10 out. 2020.

SENADO, A. **Styvenson defende princípios para uso de inteligência artificial no Brasil**. Brasília, Distrito Federal: Agência Senado, 2020 Disponível em: https://bit.ly/34Nnf9k. Acesso em: 25 out. 2020.

SIMONITE, T. **For Superpowers**: Artificial Intelligence fuels new global arms Race. Boone: Wire, Sept. 2017. Disponível em: https://www.wired.com/story/for-superpowers-artificial-intelligence-fuels-new-global-arms-race. Acesso em: 8 out. 2020.

SYMANTEC. **Cyber Security Predictions**: 2019 and beyond. Tempe: Symantec, Nov. 2018. Disponível em: https://www.symantec. com/blogs/feature-stories/cyber-security-predictions-2019-and-beyond. Acesso em: 10 out. 2020.

TAKANEN, A.; DEMOTT, J.; MILLER, C. **Fuzzing for Software Security Testing and Quality Assurance**. Boston: Artech House, 2008. E-book

TRIOLO, P.; KANIA, E. **Chinese government outlines AI ambitions through**. Washington, DC: New America, Jan. 2018. Disponível em: https://bit.ly/2GgfkHY. Acesso em: 10 out. 2020.

TYUGU, E. **Algorithms and Architectures of Artificial Intelligence**. Amsterdam: IOS Press, 2007. E-book.

VASUDEVAN, V. **How AI Is Transforming Cyber Defense**. New Jersey: Forbes, July 2018. Disponível em: https://www.forbes.com/sites/forbestechcouncil/2018/07/24/how-ai-is-transforming-cyber-defense/. Acesso em: 10 out. 2020.

VEMPATI, S. **India and the Artificial Intelligence Revolution**. Carnegie India, Aug. 2016. Disponível em: http://www.jstor.org/stable/10.2307/resrep12855. Acesso em: 10 out. 2020.

WHYTE, C. **Problems of Poison**: new paradigms and "agreed" competition in the era of AI-enabled cyber pperations. 2020 12th International Conference on Cyber Conflict (CyCon), 2020. Disponível em: http://carnegieindia.org/2016/08/11/india-and-artificial-intelligence-revolution-pub-64299. Acesso em: 21 out. 2020

*Artigo apresentado como trabalho de conclusão do Curso de Pós-graduação em Guerra Cibernética do Centro de Guerra Eletrônica do Exército Brasileiro em 2020 pelo então 1º Tenente Taffarel orientado pelo Primeiro-Sargento Comunicante Adão dos Santos, pelo Capitão-Tenente (AFN) Vanderlan Silva da Costa e pelo Prof. MSc. José Barbosa da Silva Filho.