HOPLOS
VOL. 08 Nº 14/2024

Rebeca Rabêlo

Mestranda do Programa de Pós-Graduação em Relações Internacionais da Universidade Estadual da Paraíba (PPGRI/UEPB).

Rachel Soares

Graduada em Relações Internacionais pela Universidade Estadual da Paraíba (UEPB).

AS IMPLICAÇÕES E OS DESAFIOS DA DEFESA CIBERNÉTICA EM REFERÊNCIA ÀS TECNOLOGIAS EMERGENTES

THE IMPLICATIONS AND CHALLENGES OF CYBER DEFENSE WITH REFERENCE TO EMERGING TECHNOLOGIES

RESUMO: Como as tecnologias emergentes aumentam as vulnerabilidades cibernéticas? O presente artigo tem como objetivo refletir sobre os desafios associados à utilização de novas tecnologias na defesa cibernética. Assim, este trabalho propõe um estudo exploratório que examina o rápido desenvolvimento das tecnologias emergentes e sua aplicação na defesa cibernética. O estudo é conduzido por meio de uma revisão bibliográfica abrangente, englobando teorias relevantes sobre o espaço cibernético, defesa cibernética e tecnologias emergentes. O artigo está estruturado em três seções distintas. A primeira seção explora as questões relacionadas à vulnerabilidade e ameaças no ciberespaço, delineando os desafios críticos enfrentados nesse ambiente digital. Na segunda seção, são examinados os conceitos fundamentais das tecnologias emergentes, destacando suas potenciais aplicações e implicações na segurança cibernética. Por fim, a terceira seção investiga os desafios específicos e as implicações decorrentes da integração dessas tecnologias no espaço cibernético, ao oferecer uma análise aprofundada de seu impacto e relevância para a defesa cibernética contemporânea.
Palavras-Chave: Segurança; Tecnologias; Ciberespaço; Defesa.

ABSTRACT: How do emerging technologies increase cyber vulnerabilities? This article aims to reflect on the challenges associated with the use of new technologies in cyber defense. Thus, this article proposes an exploratory study that examines the rapid development of emerging technologies and their application in cyber defense. The study is conducted through a comprehensive literature review, encompassing relevant theories on cyberspace, cyber defense and emerging technologies. The article is structured in three distinct sections. The first section explores the issues related to vulnerability and threats in cyberspace, outlining the critical challenges faced in this digital environment. The second section examines the fundamental concepts of emerging technologies, highlighting their potential applications and implications for cyber security. Finally, the third section investigates the specific challenges and implications arising from the integration of these technologies into cyberspace, offering an in-depth analysis of their impact and relevance to contemporary cyber defense.
Keywords: Security; Technologies; Cyberspace; Defense.

1 Introdução

No contexto contemporâneo, torna-se cada vez mais evidente a interdependência entre os avanços tecnológicos e a crescente fragilidade do espaço cibernético. A revolução digital tem proporcionado uma gama de benefícios, mas também revelou um território virtual suscetível a ameaças e ataques de diversas naturezas, como obtenção de informações sensíveis, crimes cibernéticos e operações de inteligência utilizando *Big Data* (VALERIANO, MANESS, 2018; PORTELA, 2018; DOUZET, 2014). Dessa forma, o desenvolvimento de tecnologias emergentes e a exposição a vulnerabilidades cibernéticas apresentam desafios inéditos para o cenário internacional.

A complexidade e a interconectividade dessas tecnologias aumentam a superfície de ataque, tornando-as alvos atraentes para cibercriminosos e agentes mal-intencionados. Além disso, a dificuldade de identificar e corrigir todas as falhas de segurança durante o processo de desenvolvimento faz com que a mitigação desses riscos seja extremamente desafiadora. Como resultado, a implementação de medidas de segurança eficazes torna-se crucial para proteger tanto os dados pessoais quanto a infraestrutura crítica contra possíveis explorações e ataques cibernéticos.

Diante disso, o presente artigo pretende analisar como as tecnologias emergentes aumentam as vulnerabilidades cibernéticas. Tendo como objetivo refletir sobre os desafios associados à utilização de novas tecnologias na defesa cibernética. Visto que, diante do crescimento da infraestrutura de rede e a quantidade de dispositivos conectados, surgem oportunidades para invasões devido a vulnerabilidades, enquanto a intensa troca de dados entre os indivíduos na Internet aumenta o risco de exploração e manipulação de informações.

Para atender ao objetivo proposto, optou-se pela abordagem qualitativa. Assim, este artigo propõe um estudo exploratório que examina o rápido desenvolvimento das tecnologias emergentes e sua aplicação na defesa cibernética. O estudo é conduzido por meio de uma revisão bibliográfica abrangente, englobando teorias relevantes sobre o espaço cibernético, defesa cibernética e tecnologias emergentes. Os procedimentos incluem a identificação de fontes primárias e secundárias, a revisão detalhada da literatura pertinente à temática, o que proporciona uma análise ampla do desenvolvimento das tecnologias emergentes e sua aplicação na defesa cibernética.

O artigo está estruturado em três seções distintas. A primeira seção explora as questões relacionadas à vulnerabilidade e ameaças no ciberespaço, delineando os desafios críticos enfrentados nesse ambiente digital. Na segunda seção, são examinados os conceitos

fundamentais das tecnologias emergentes, destacando suas potenciais aplicações e implicações na segurança cibernética. Por fim, a terceira seção investiga os desafios específicos e as implicações decorrentes da integração dessas tecnologias no espaço cibernético, ao oferecer uma análise aprofundada de seu impacto e relevância para a defesa cibernética contemporânea.

2 Vulnerabilidade e ameaças no espaço cibernético

As tecnologias emergentes e as novas tendências de gestão estão continuamente reformulando o panorama da cibersegurança. Tradicionalmente, os Estados eram definidos por regiões físicas e territórios claramente demarcados. No entanto, o ciberespaço ultrapassa essas fronteiras convencionais (POHLE, VOELSEN, 2022). No ambiente cibernético, a capacidade dos Estados de regulamentar e controlar é significativamente reduzida, pois tanto atores estatais quanto não estatais operam de maneira autônoma (AYRES PINTO, FREITAS, PAGLIARI, 2018). Segundo Stiennon (2015), os ataques cibernéticos aumentaram a conscientização sobre as ameaças à segurança nacional, uma vez que o ciberespaço pode causar danos graves em domínios geográficos tradicionais.

De acordo com Assis, Bittencourt e Tavares (2020), a securitização e politização do espaço cibernético tornam suas operações de grande interesse e promovem mudanças significativas no setor militar. Visto que, a revolução da informação influencia de forma decisiva as operações militares devido ao desenvolvimento contínuo de tecnologias que tornam a sociedade e os governos cada vez mais dependentes de serviços digitais em infraestruturas críticas (ASSIS, BITTENCOURT, TAVARES, 2020; CAVELTY, 2012).

Assim, as ameaças e vulnerabilidades cibernéticas variam de acordo com as capacidades relativas e absolutas dos envolvidos. A interconectividade global gera vulnerabilidades, especialmente para aqueles que dependem intensamente de sistemas cibernéticos, amplificando a percepção de ameaças (CHOUCRI, 2012). As desigualdades tecnológicas criam assimetrias, permitindo que atores mais avançados explorem as vulnerabilidades dos menos capacitados, resultando em percepções desequilibradas de ameaças cibernéticas (STIENNON, 2015). A avaliação das operações neste domínio deve ser multifacetada e inovadora, incorporando diversas áreas do conhecimento para uma compreensão abrangente.

A Doutrina Conjunta Aliada para as Operações no Ciberespaço (CO), publicada pela OTAN em janeiro de 2020, reflete sobre a necessidade de gestão de um sistema dinâmico e complexo, capaz de prever e prevenir ciberataques em tempo real:

> A liberdade de ação no ciberespaço pode ser tão crucial quanto o controle sobre a terra, o ar, o espaço ou o mar. Em um ambiente cada vez mais interconectado, é mais difícil distinguir entre os níveis estratégico, operacional e tático[…] Sendo o ciberespaço um domínio de operações, é necessária uma mudança operacional para focar na garantia da missão (OTAN, 2020).

As tecnologias emergentes trazem novas oportunidades para melhorar a cibersegurança, mas também introduzem riscos inéditos, pois as tecnologias de informação e comunicação estão profundamente integradas na sociedade, desde computadores pessoais até Infraestruturas Críticas[1] que dependem do funcionamento remoto de redes (por exemplo, eletricidade, redes de esgoto, sistema financeiro) (ASSIS, BITTENCOURT, TAVARES, 2020). Portanto, a integração dessas tecnologias deve ser gerenciada de forma cuidadosa para assegurar a segurança e a resiliência cibernética em todos os níveis. Para enfrentar as ameaças cibernéticas em constante evolução, investir em cibersegurança, fomentar a inovação e a colaboração são medidas essenciais para proteger os ativos digitais e garantir a segurança e a continuidade operacional em um mundo cada vez mais interconectado e orientado por dados. A partir disso, é possível explorar de forma mais detalhada como as tecnologias emergentes podem ser aproveitadas para fortalecer ainda mais a segurança cibernética e impulsionar a inovação.

3 Tecnologias emergentes e suas possibilidades

Nos últimos anos, as tecnologias emergentes têm se tornado tema central, tanto na pesquisa acadêmica quanto nas agendas políticas, refletindo um crescente interesse e reconhecimento de seu potencial transformador. Este fenômeno é evidenciado pelo aumento significativo no número de publicações e artigos que abordam esse tema (ROTOLO, HICKS, MARTIN, 2015). No entanto, apesar do interesse crescente, há uma falta de consenso sobre o que define uma tecnologia como emergente, sendo considerado um termo em *constructo*. Este debate revela a natureza complexa e em constante evolução do conceito de tecnologia emergente, que pode ser influenciado por fatores como novidade, potencial disruptivo e disponibilidade comercial.

Além disso, a compreensão das tecnologias emergentes varia dependendo da perspectiva analítica, o que tem levado ao desenvolvimento de uma ampla gama de abordagens metodológicas para detectar e analisar sua emergência. Diante desse contexto dinâmico, é

[1] Para Mandarino Júnior (2010, p. 38), as "Infraestruturas Críticas são instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional e à segurança do Estado e da sociedade".

crucial explorar tanto as oportunidades quanto os desafios apresentados pelas tecnologias emergentes, especialmente no que diz respeito à segurança cibernética.

De acordo com os autores Day e Schoemaker (2000), Srinivasan (2008), as tecnologias emergentes são inovações de base científica com potencial para criar um novo setor ou transformar um já existente. Por exemplo, as editoras discográficas e o mercado de DVD foram destruídos devido ao aparecimento do sistema de *streaming*. A utilização da palavra "ciência" significa que as tecnologias emergentes são produzidas a partir da colaboração da investigação e do desenvolvimento, uma vez que a maioria delas começa como uma ideia conceitual de investigação antes de serem criadas e desenvolvidas.

> Uma tecnologia ainda está emergindo se ainda não for um "must-have". Por exemplo, há alguns anos, o correio eletrônico era uma tecnologia opcional. De fato, a sua eficácia como ferramenta de comunicação era limitada quando apenas algumas pessoas de uma organização tinham acesso regular a ele. Atualmente, é uma tecnologia imprescindível e de utilização obrigatória para a maioria das pessoas na maioria das organizações. Neste sentido, uma tecnologia pode ser uma expectativa padrão no mundo comercial ou empresarial, embora ainda seja considerada "emergente" (MILLER; GREEN; PUTLAND, 2005, p. 6).

A definição fornecida anteriormente enfoca a utilização da tecnologia dentro de um contexto específico ou domínio. Esta definição também está alinhada com a perspectiva de Daniel *et al.* (1998), que consideram essas tecnologias inovadoras como aquelas em que estão disponíveis no setor econômico, porém ainda foram adotadas de forma geral, ou aquelas que podem se tornar disponíveis no ambiente comercial nos próximos cinco anos. Essa abordagem sugere que uma tecnologia não precisa ser nova para ser classificada como emergente.

A compreensão das tecnologias emergentes também depende da perspectiva da análise, por exemplo, um analista pode considerar uma tecnologia emergente devido à sua novidade e ao impacto socioeconômico esperado, enquanto outros podem ver a mesma tecnologia como uma extensão natural de uma tecnologia existente (GLÄNZEL, THIJS, 2012). Com isso, foram desenvolvidas várias abordagens metodológicas para a detecção e análise da emergência nos domínios da ciência e da tecnologia.

Estes métodos, favorecidos por tirarem partido do crescente poder computacional e de novos conjuntos de dados de grande dimensão e por permitirem trabalhar com indicadores e modelos mais sofisticados, carecem de fortes ligações a conceitos bem pensados, sendo assim, há uma dificuldade na produção de uma definição do conceito central de uma tecnologia emergente (BOYACK *et al*., 2014). Por conseguinte, aponta-se que as abordagens à detecção e

análise da emergência tendem a ser muito diferentes, mesmo com a utilização dos mesmos ou de métodos semelhantes.

Assim, tecnologias emergentes como *Blockchain,* Internet das Coisas e Inteligência Artificial continuam a moldar o cenário da segurança cibernética, sendo fundamental reconhecer a complexidade e a diversidade das ameaças e defesas associadas a essas inovações (MANDAL, SINGHAL, TYAGI, 2023). Embora ofereçam inúmeras oportunidades para melhora da sociedade, governos e negócios, também apresentam novos desafios e riscos que exigem uma resposta proativa e robusta. Portanto, é imperativo que, ao adotar essas tecnologias, também sejam incorporadas medidas de segurança desde o início do processo de implementação. A integração cuidadosa de tecnologias emergentes na infraestrutura de segurança cibernética não apenas fortalecerá nossa resiliência digital, mas também nos permitirá aproveitar ao máximo seu potencial inovador de maneira segura e responsável. Neste contexto, os próximos tópicos abordam em detalhes essas tecnologias emergentes e suas implicações para a segurança cibernética.

3.1 *Blockchain*

Desde que a moeda digital criptográfica, denominada *Bitcoin,* surgiu em 31 de outubro de 2008 (NAKAMOTO, 2008), um leque diversificado de investigadores e profissionais têm dedicado um interesse considerável à tecnologia *Blockchain*. A tecnologia *Blockchain* funciona como o livro-razão, que é um livro contábil que permite o controle individualizado das movimentações das contas empresariais, utilizado para registar todas as transações de *Bitcoin* (FANNING, CENTERS, 2016). Os registos das transações tornam-se públicos de forma justa no âmbito da cadeia de blocos, pondo à prova o aspecto da privacidade. Pois, todos os intervenientes no ambiente tecnológico empresarial moderno poderiam verificar os pormenores das transações, uma vez que o atual sistema bancário tradicional mantém esta forma de privacidade por meio da manutenção de registros confidenciais.

A cadeia de blocos (*blockchain*) é definida, grosso modo, como um conjunto de blocos ligados individualmente, cada um compreendendo várias transações que produzem um armazenamento de dados distribuído que pode ser utilizado numa vasta gama de aplicações (FANNING, CENTERS, 2016), incluindo votação eletrônica, financiamento coletivo, recursos distribuídos, gestão de registros públicos e gestão de identidades. Segundo Yli-Huumo *et al.* (2016), as transações monetárias entre indivíduos ou organizações são normalmente consolidadas e geridas por uma empresa terceirizada.

A *Blockchain* permite que a tecnologia atue como a força motriz da próxima revolução vital na perspectiva das tecnologias da informação. Várias implementações da tecnologia *Blockchain* são utilizadas nos negócios modernos e cada implementação tem a sua força distinta em vários setores, desde a Internet das Coisas (IoT) e finanças, até à gestão da cadeia de abastecimento, cuidados de saúde e sistemas de reputação (PANARELLO *et al*., 2018; FANNING, CENTER, 2016; ESPOSITO *et a*l., 2018; KSHETRI, 2018; DENNIS, OWEN, 2015). A incorporação de transações comerciais, a segurança da informação, a privacidade e a garantia de segurança num ambiente em linha tornaram-se necessárias para melhorar a produção.

A utilização das tecnologias da informação e da comunicação tem possibilitado o crescimento econômico (FARHADI *et a*l., 2012). Houve um crescimento de debates que se propõem analisar a efetividade da tecnologia *Blockchain* no que tange a resolução da segurança e privacidade das transações. Gupta e Dubey (2016), explicam que a privacidade, a segurança e a confiança são questões fundamentais para as tecnologias eletrônicas atualmente e que a segurança do comércio eletrônico é fundamental para os componentes que influenciam o comércio eletrônico, como a segurança dos dados, a integridade, a privacidade e outras áreas mais amplas do contexto da segurança da informação.

3.2 *Internet das Coisas (IoT)*

A Internet das Coisas (IoT) criou um novo paradigma em que uma rede de máquinas e dispositivos capazes de comunicar e colaborar entre si está a impulsionar inovações nos processos das empresas (LEE, 2019). Os ataques generalizados e cada vez mais frequentes à cibersegurança dos sistemas IoT têm causado às pessoas e às organizações uma vasta gama de problemas de reputação, conformidade, finanças e operações comerciais. O rápido aumento dos ciberataques deve-se, em parte, ao crescimento fenomenal dos dispositivos IoT em domínios, como as redes inteligentes, a monitorização ambiental, os sistemas de monitorização de doentes, a fabricação inteligente e a logística. A gestão da segurança da Internet das coisas é um desafio devido à natureza dinâmica e transitória da ligação entre dispositivos (ATZORI *et. al.*, 2010), à diversidade de atores capazes de interagir nos sistemas IoT (NURSE *et al*., 2017) e às limitações de recursos (MALIK, SINGH, 2019).

Estão constantemente surgindo novas tecnologias para lidar com os desafios no espaço cibernético que oferecem oportunidades e desafios para a gestão de riscos e ameaças da IoT. Segundo Sha *et al*. (2018), o objetivo da cibersegurança da IoT é reduzir o risco para as

organizações e os usuários por meio da proteção dos bens da IoT e da privacidade. A maioria dos estudos anteriores centram-se nos aspectos tecnológicos da cibersegurança da IoT. No entanto, faltam quadros de gestão de riscos abrangentes para abordar as complexas questões de cibersegurança nos sistemas IoT (O'NEILL *et al*., 2016). A falta de segurança nos sistemas IoT abre oportunidades para que intrusos e *hackers*[2] acessem infraestruturas críticas e dados sensíveis. No entanto, para Sicari (2015), a ausência de um quadro de gestão do risco de cibersegurança da IoT torna muito difícil para as organizações tomarem decisões eficazes sobre a gestão do risco e o investimento na cibersegurança da IoT.

3.3 *Inteligência Artificial*

O termo inteligência artificial (IA), cunhado nos anos 50, é o domínio da informática que mostra os programas destinados a modelar o "inteligência". Isto, na prática, significa algoritmos que podem aprender ou raciocinar, dado o conhecimento de base e os *inputs* necessários, e são utilizados para tarefas, por exemplo, a tomada de decisões autônomas, o reconhecimento e o planejamento.

Para Brundage *et al*. (2018), um dos principais riscos de segurança dos sistemas de inteligência artificial é o potencial de um invasor comprometer a integridade do processo de tomada de decisão, de modo que as escolhas não sejam feitas conforme esperado ou pretendido pelo designer. Uma maneira de conseguir isso é fazer com que o adversário assuma o controle direto do sistema de IA, permitindo que o sistema decida o que produzir e quais decisões tomar. Como alternativa, um invasor pode tentar influenciar essas decisões de maneira mais sutil e indireta, alimentando o modelo de IA com entrada maliciosa ou dados de treinamento.

Por exemplo, um adversário tentando danificar um veículo autônomo para aumentar a probabilidade de um acidente pode explorar vulnerabilidades no *software* do carro para tomar decisões de direção. Para Yampolskiy e Spellchecker (2018), no entanto, acessar e explorar remotamente o *software* que executa um veículo pode ser difícil, desta forma, um invasor pode pintar um veículo com tinta para fazê-lo ignorar os sinais de parada. Com isso, aponta-se que os algoritmos de visão computacional não podem reconhecê-lo como um sinal de parada. O processo pelo qual os adversários podem manipular dados de entrada para interromper os sistemas de IA é chamado de aprendizado de máquina adversário.

[2] Para Levy (2001), *hacker* é um indivíduo capaz de invadir dispositivos eletrônicos, redes e sistemas de computação, seja para verificar sua segurança, para aperfeiçoá-lo ou para praticar atos ilícitos.

Os pesquisadores descobriram que mesmo pequenas mudanças em uma imagem digital imperceptível ao olho humano podem fazer com que os algoritmos[3] de inteligência artificial classifiquem completamente essa imagem (STOICA *et al*., 2017). Esses riscos falam da necessidade de um controle cuidadoso sobre os conjuntos de dados de treinamento usados para criar modelos de IA e as entradas fornecidas a esses modelos para garantir a segurança dos processos de tomada de decisão habilitados para aprendizado de máquina.

A Comissão de Segurança Nacional dos EUA sobre Inteligência Artificial (NSCAI) enfatizou a importância de criar sistemas de IA confiáveis, que possam ser verificados usando um sistema de documentação rigoroso e padronizado. Para esse fim, o comitê recomenda o desenvolvimento de processos e padrões abrangentes de documentação de design para modelos de inteligência artificial, incluindo os dados usados pelo modelo, parâmetros e pesos do modelo, treinamento e teste do modelo e saída do modelo (NSCAI, 2020).

Para muitos governos, o próximo passo nas considerações de segurança da IA é descobrir como implementar as ideias de transparência, auditoria e responsabilidade para abordar com eficácia os riscos de processos inseguros de tomada de decisões de IA e padrões de exfiltração de dados. Conforme a proposta da NSCAI, os sistemas de IA devem desenvolver processos de documentação mais abrangentes para garantir a transparência. A documentação rigorosa de como o modelo foi desenvolvido e testado e os resultados resultantes permitem que os especialistas identifiquem lacunas nas habilidades, manipulação potencial de entradas ou dados de treinamento e resultados inesperados (NSCAI, 2020).

Um ponto interessante para os investimentos em investigação para a cibersegurança é aplicar sistemas de IA em áreas de infraestruturas críticas para resolver os desafios persistentes da cibersegurança, o que incluem a monitorização da rede para técnicas de análise de *software*, a detecção de anomalias para identificar as vulnerabilidades do código e sistemas de raciocínio cibernéticos para sintetizar correções defensivas até a primeira indicação de um ataque (VERMA, GUPTA, 2020; BRESNIKER *et al*., 2019). Os sistemas de IA podem efetuar estas análises em segundos em vez de semanas ou dias, dessa forma os ciberataques poderiam ser defendidos e observados no momento em que ocorrem. Mas, conforme explica Bresniker *et al.* (2019), seria necessária uma implantação segura para compreender as implicações de várias dimensões e destas ações de IA.

[3] Para Manzano e Oliveira (2016, p. 25) algoritmo pode ser compreendido como "regras formais, sequenciais e bem definidas a partir do entendimento lógico de um problema a ser resolvido por um programador com o objetivo de transformá-lo em um programa que seja possível ser tratado e executado por um computador."

A IA pode ser utilizada pela cibersegurança para aumentar a consciência, reagir em tempo real e melhorar a sua eficácia global, o que inclui ajustamento e autoadaptação contra os ataques contínuos que alteram as irregularidades existentes entre atacantes e defensores (CALDERON, 2019). Estratégias que ajudam a identificar os pontos fracos do adversário, utilizando métodos de observação e recolhendo lições aprendidas, podem utilizar a IA para categorizar vários tipos de ataques, além de informar a resposta adaptativa em escala, por exemplo, encontrar inconsistências e saber como reparar (PATIL, 2016).

3.4 *5G*

Nas gerações anteriores de conectividade, o 3G desempenhou um papel fundamental na democratização do uso da internet móvel e na facilitação da navegação na web, acesso a e-mail e compartilhamento de fotos. Por outro lado, o 4G pode criar novos serviços relacionados à mobilidade urbana por meio de plataformas de streaming de vídeo e áudio e elevar e entregar entretenimento em dispositivos móveis (GOMES, 2018). Em uma evolução contínua, o 5G representa um ponto de virada na mudança do mundo como o conhecemos. Segundo Rajasekar *et al*. (2022), a conectividade e compatibilidade com o conceito de Internet das Coisas impactará diversos setores como saúde, obras públicas, mobilidade urbana, agronegócio, logística e telecomunicações. Além de mudar a arquitetura das cidades, casas, economias e o cotidiano das pessoas.

As redes 5G são uma parte importante do design de veículos autônomos que aprimoram a inteligência artificial (IA), geram informações em tempo real no contexto e reduzem o tempo de resposta. Na telemedicina, o 5G permitirá que os médicos realizem alguns procedimentos mesmo quando estiverem longe dos pacientes. Modelos de negócios, escritórios e fluxos de trabalho serão repensados. Além de otimizar as indústrias existentes, o 5G facilitará o surgimento de novos modelos de negócios e formas de comunicação (SHARMA, JHA, 2021).

Para Rajasekar *et al*. (2022), um dos aspectos mais importantes do 5G é o crescente desenvolvimento de dispositivos integrados para conceitos de Internet das Coisas. Além disso, haverá uma integração em que produtos de todos os tipos funcionarão online, criando uma vasta rede unificada. Casas automatizadas terão mais energia quando eletrônicos de *smartphones* a televisores, *laptops*, geladeiras, aspiradores de pó, condicionadores de ar e máquinas de lavar forem conectados como um sistema.

Apesar das promessas da tecnologia 5G, ela abre portas para desafios e questões abertas a serem enfrentadas. A segurança é o principal problema enfrentado pelas redes 5G, o que afeta

a privacidade do usuário e a segurança do sistema. Desde o início, as redes de comunicação sem fio sempre estiveram expostas a vulnerabilidades de segurança. Sendo alvo de diferentes ataques ao longo da evolução da rede sem fio desde sua primeira geração. Com o 5G, os ataques existentes se fortalecem e novos ataques surgirão das principais tecnologias facilitadoras, conforme mencionado anteriormente. Portanto, mais esforços precisam ser focados nos desafios de segurança enfrentados pelas redes 5G e como eles podem ser mitigados (CABAJ *et al*., 2018).

Para Brunner (2021), os principais desafios de segurança no 5G incluem mais segurança necessária para garantir a segurança da infraestrutura de rede crítica e a privacidade do usuário em um ambiente altamente conectado, onde tudo está conectado à Internet e exposto a diferentes ataques. Por exemplo, uma falha de segurança em um dos sistemas de rede inteligente pode levar a danos no sistema elétrico e, portanto, na cidade inteligente que depende dele. A consequência da violação de segurança pode se espalhar facilmente pela rede conectada para prejudicar outros sistemas e outros serviços.

4 Desafios e implicações das tecnologias emergentes para defesa cibernética

As tecnologias podem ser definidas como o conjunto de conhecimentos teóricos e práticos, competências e artefatos utilizados para desenvolver, produzir e fornecer produtos e serviços (BURGELMAN, ROSENBLOOM, 1989). Essa definição aplica-se tanto à tecnologia empresarial quanto à militar. Conforme destaca Grissom (2006), a tecnologia militar combina conhecimentos teóricos e práticos, bem como o conhecimento individual e coletivo, que surgem no contexto da defesa por meio da aprendizagem prática, do trabalho em equipe, da cultura e de bens tangíveis, como equipamentos e instalações de fabricação.

De acordo com essa definição, grande parte da tecnologia de base que sustenta a defesa é tangível e humana. A distinção está entre tecnologias e produtos/serviços, no caso militar, refere-se às armas, seus sistemas de distribuição e a infraestrutura que suporta a capacidade militar. As tecnologias são fundamentais para os sistemas de armamento, mas são distintas deles. Segundo Grissom (2006), os militares buscam capacidades, não tecnologias em si. Consequentemente, a combinação de tecnologias emergentes e outros fatores para formar a capacidade militar é crítica, e não as tecnologias emergentes por si só.

As tecnologias emergentes podem ter implicações significativas para a capacidade militar, mas o caminho desde a emergência tecnológica até a capacidade militar é longo e incerto (GOLDMAN, ELIASON, 2003). A agilidade e capacidade de resposta do processo de

aquisição às novas tecnologias são extremamente importantes. Igualmente relevante é o reconhecimento de que a combinação de tecnologias maduras em uso também pode ter profundas implicações na capacidade militar (GOLDMAN, ELIASON, 2003). Surge, então, a questão de se devemos utilizar uma medida absoluta ou relativa para avaliar se uma tecnologia é "emergente".

O que é uma tecnologia aprofundada em um Estado pode ser emergente em outro. Isso levanta questionamentos importantes sobre a difusão de tecnologias e inovações militares no cenário internacional (JAMES, 2016). As transferências de armamento e a cooperação desempenham um papel crucial nesse processo, especialmente à medida que governos e empresas da Europa, dos EUA e outros países buscam participação nos crescentes orçamentos de defesa da Ásia-Pacífico (GOLDMAN, ELIASON, 2003).

Segundo Yedugondla (2022), essas tecnologias transformarão radicalmente a maneira como as pessoas trabalham, comunicam, pensam e até lutam no futuro próximo, gerando preocupações sobre interferências e perturbações de atores estatais em redes vitais. Satisfazer as exigências de segurança essenciais, especialmente sob uma perspectiva militar, enquanto se aproveitam as capacidades das múltiplas nuvens, pode ser desafiador. As cadeias de abastecimento dos setores aeroespacial e de defesa podem se beneficiar dos serviços multinuvem, envolvendo diferentes contratantes de defesa, extraindo dados de múltiplas fontes e fornecendo-os a um único local e aplicação (OTAN, 2023).

As implicações das tecnologias emergentes para o combate e a estabilidade estratégica são difíceis de prever, pois dependem de diversos fatores, como o ritmo de desenvolvimento tecnológico, a integração dessas tecnologias nas forças militares e conceitos operacionais existentes, e as políticas nacionais e internacionais que facilitam ou inibem seu desenvolvimento e uso (JAMES, 2016). Muitas tecnologias emergentes têm características que podem potencialmente alterar a natureza da guerra. Por exemplo, tecnologias como a IA, análise de grandes volumes de dados e armas autônomas letais podem reduzir a necessidade de operadores humanos (WORK, BRIMLEY, 2014).

O que pode aumentar a eficiência e acelerar o ritmo dos combates, possivelmente com consequências desestabilizadoras. Tecnologias emergentes, como drones de baixo custo, podem mudar o equilíbrio entre a qualidade das forças militares e a quantidade, bem como entre ofensiva e defensiva (JAMES, 2016). Enxames de veículos não tripulados coordenados podem sobrecarregar sistemas defensivos, favorecendo o atacante, enquanto armas de energia dirigida

podem neutralizar esses ataques, beneficiando o defensor (SCHARRE, 2016). Assim, o equilíbrio entre ataque e defesa pode mudar diversas vezes nas próximas décadas.

Dessa forma, as interações entre tecnologias emergentes podem aprimorar capacidades militares existentes ou criar novas com consequências imprevistas (SCHARRE, 2016). Por exemplo, a IA combinada com computação quântica pode produzir métodos mais poderosos de aprendizagem automática, ao melhorar o reconhecimento de imagens e identificação de alvos, permitindo armas autônomas mais sofisticadas. Hoehn e Sayler (2021) apontam que a IA combinada com tecnologias de comunicação 5G pode possibilitar ambientes de treino virtuais ou interfaces cérebro-computador para melhorar a cognição humana e controlar próteses ou sistemas robóticos.

Porém, especialmente sistemas complexos como IA, podem gerar consequências indesejadas se seu desempenho não for o esperado. Essas consequências podem variar desde falhas sistêmicas até violações da lei dos conflitos armados (DOCHERTY, 2018). Em casos extremos, uma arma autônoma pode continuar a atingir alvos inadequados até esgotar sua munição, resultando em fratricídio ou baixas civis (SCHARRE, LAMBERTH, 2022).

Além disso, é crucial considerar o impacto dessas tecnologias na dinâmica geopolítica global. A corrida tecnológica entre grandes potências, como Estados Unidos, China e Rússia, pode intensificar a competição estratégica, o que leva a novas formas de rivalidade e aumentando o risco de conflitos (SCHMITT, 2018; STIENNON, 2015; CHOUCRI, 2012). De acordo com Rid (2014), a superioridade tecnológica pode ser vista não apenas como uma vantagem militar, mas também como um instrumento de poder e influência internacional. A capacidade de desenvolver, implementar e exportar tecnologias avançadas pode redefinir alianças e adversidades ao equilíbrio de poder global.

Em resumo, as tecnologias emergentes estão redefinindo os parâmetros da guerra e da segurança global. Desde a transformação dos sistemas de armamento até as complexas implicações éticas e geopolíticas, a evolução tecnológica apresenta tanto oportunidades quanto desafios (TEIXEIRA JÚNIOR, VILAR-LOPES, FREITAS, 2017). A capacidade de adaptação e inovação será crucial para os países que desejam manter uma vantagem estratégica em um mundo cada vez mais tecnológico. A colaboração internacional, o desenvolvimento de normas e a implementação de medidas de controle serão essenciais para mitigar os riscos e maximizar os benefícios dessas tecnologias emergentes no cenário militar global.

5 Considerações Finais

Com base na análise das definições e implicações das tecnologias emergentes no contexto militar, podemos concluir que estas desempenham um papel crucial na transformação da capacidade e estratégia de defesa contemporânea. A introdução de tecnologias emergentes, como Inteligência Artificial, drones de baixo custo e armas de energia dirigida, tem o potencial de alterar significativamente o equilíbrio entre ofensiva e defensiva, qualidade e quantidade das forças militares. No entanto, o caminho desde a emergência tecnológica até a plena capacidade militar é longo e incerto, destacando a importância da agilidade e capacidade de resposta no processo de aquisição de novas tecnologias.

Dessa forma, o artigo oferece uma contribuição significativa para o entendimento das interseções entre segurança cibernética e tecnologias emergentes, destacando a importância de abordar essas questões de forma proativa e estratégica para garantir a resiliência e a segurança dos sistemas digitais no mundo moderno. As preocupações éticas e as consequências indesejadas das tecnologias emergentes, especialmente em sistemas complexos como IA, são questões críticas que precisam ser abordadas. O uso de armas autônomas e biotecnologias levanta debates sobre moralidade e legalidade, além de implicações potencialmente desestabilizadoras para a estabilidade estratégica. A interação dessas tecnologias com fatores geopolíticos e a corrida tecnológica entre grandes potências também intensificam a competição estratégica, ao redefinir alianças e adversidades.

Por fim, a transformação tecnológica está redefinindo os parâmetros da guerra e da segurança global. A capacidade de adaptação e inovação será crucial para os países que desejam manter uma vantagem estratégica em um mundo cada vez mais tecnológico. A colaboração internacional, o desenvolvimento de normas e a implementação de medidas de controle serão essenciais para mitigar os riscos e maximizar os benefícios das tecnologias emergentes no cenário militar global. Em um ambiente em que as mudanças tecnológicas ocorrem em um ritmo acelerado, a preparação e a resposta adequadas determinarão o sucesso ou o fracasso das nações na manutenção de sua segurança e soberania.

Referências

ASSIS, A. C. de O.; BITTENCOURT, N. V.; TAVARES, S. M. B. Armas inteligentes no ciberespaço: oportunidades inovadoras e desafios prementes. *Revista Brasileira de Estudos de Defesa*, *[S. l.]*, v. 7, n. 2, 2021. DOI: 10.26792/rbed.v7n2.2020.75211. Disponível em: https://rbed.abedef.org/rbed/article/view/75211. Acesso em: 27 maio 2024.

ATZORI, L.; IERA, A.; MORABITO, G. The internet of things: A survey. *Computer networks*, v. 54, n. 15, p. 2787-2805, 2010. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cs.mun.ca/courses/cs6910/IoT-Survey-Atzori-2010.pdf. Acesso em: 5 de maio 2023.

AYRES PINTO, D.; FREITAS, R. V.; PAGLIARI, G. 2019. Fronteiras virtuais: Um debate sobre segurança e soberania do Estado. In: Danielle Jacon Ayres Pinto, Maria Freire e Daniel Chaves (eds). *Fronteiras Contemporâneas Comparadas: Desenvolvimento, Segurança e Cidadania*. Macapá: Editora da Universidade Federal do Amapá, pp. 39-52, 2019.

BOYACK, K.; SMALL, H.; KLAVANS, R. Improving the accuracy of co-citation clustering using full text. *Journal of the American Society for Information Science and Technology*, vol. 64, n. 9, p. 1759-1767, 2013. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/asi.22896. Acesso em: 5 de junho 2023.

BRESNIKER, Kirk *et al*. Grand challenge: Applying artificial intelligence and machine learning to cybersecurity. *IEEE explore*, v. 52, n. 12, p. 45-52, 2019. Disponível em: https://ieeexplore.ieee.org/document/8909930?utm_source=researcher_app&utm_medium=referral&utm_campaign=RESR_MRKT_Researcher_inbound. Acesso em: 15 de junho 2023.

BRUNDAGE, Miles *et al*. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*, 2018. Disponível em: https://www.researchgate.net/publication/323302750_The_Malicious_Use_of_Artificial_Intelligence_Forecasting_Prevention_and_Mitigation. Acesso em: 1 de abril 2023.

BRUNNER, T. Cybersecurity in beyond 5G: use cases, current approaches, trends, and challenges. *Communication Systems XIV*, p. 28, 2021. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://files.ifi.uzh.ch/CSG/teaching/FS21/IFI_2021_02.pdf. Acesso em: 13 de abril 2023.

BURGELMAN, R. A.; ROSENBLOOM, R. S. Technology strategy: an evolutionary process perspective. *Research on technological innovation, management and policy*, v. 4, n. 1, p. 1-23, 1989. Disponível em: https://www.econbiz.de/Record/technology-strategy-an-evolutionary-process-perspective-burgelman-robert/10001090017. Acesso em: 15 de abril de 2023.

BUZAN, B.; WÆVER, O.; DE WILDE, J. *Security: A new framework for analysis*. Lynne Rienner Publishers, 1998.

CABAJ, Krzysztof *et al*. Cybersecurity: trends, issues, and challenges. *EURASIP Journal on Information Security,* vol. 10, n. 1, 2018. Disponível em: https://jis-

eurasipjournals.springeropen.com/articles/10.1186/s13635-018-0080-0#citeas. Acesso em: 15 de abril de 2023.

CALDERON, R. The benefits of artificial intelligence in cybersecurity. *Economic Crime Forensics Capstones*, n. 36, 2019. Disponível em: https://digitalcommons.lasalle.edu/ecf_capstones/36/. Acesso em: 25 de abril de 2023.

CAVELTY, Myriam Dunn. The Militarisation of Cyber Security as a Source of Global Tension: strategic trends analysis. *Strategic Trends Analysis*, [*s. l*], p. 103-124, 18 fev. 2012. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2007043. Acesso em: 27 maio 2024.

CHOUCRI, Nazli. *Cyberpolitics in International Relations*. London: The Mit Press, 2012. 320 p. Acesso em: Disponível em: https://mitpress.mit.edu/9780262517690/cyberpolitics-in-international-relations/. Acesso em: 25 de julho de 2023.

DANIEL *et al*. *Technical Assessment of Residential and Small Commercial Emerging Technologies*. San Francisco, CA: Pacific Gas & Electric Company, 1998.

DAY, G. S.; SCHOEMAKER, P. J. H. Avoiding the pitfalls of emerging technologies. *California management review*, v. 42, n. 2, p. 8-33, 2000. Disponível em: https://www.researchgate.net/publication/243768097_Avoiding_the_Pitfalls_of_Emerging_Technologies. Acesso em: 20 de junho 2023.

DENNIS, R.; OWEN, G. Rep on the block: A next generation reputation system based on the blockchain. In: *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 2015. p. 131-138. Disponível em: https://ieeexplore.ieee.org/document/7412073. Acesso em: 10 de junho 2023.

DOCHERTY, B. L. *Heed the Call: A Moral and Legal Imperative to Ban Killer Robots*. [s.l.] Human Rights Watch, 2018. Disponível em: https://books.google.com.br/books/about/Heed_the_Call.html?id=4QNcuwEACAAJ&redir_esc=y. Acesso em: 24 de abril 2023.

DOUZET, F. La géopolitique pour comprendre le cyberespace. *Hérodote*, [S.L.], v. 152-153, n. 1, p. 3-21, 1 jun. 2014. CAIRN. http://dx.doi.org/10.3917/her.152.0003. Disponível em: https://www.cairn-int.info/article-E_HER_152_0003--understanding-cyberspace-with-geopolitic.htm. Acesso em: 25 abr. 2023.

ESPOSITO, Christian *et al*. Blockchain: A panacea for healthcare cloud-based data security and privacy?. *IEEE cloud computing*, v. 5, n. 1, p. 31-37, 2018. Disponível em: https://ieeexplore.ieee.org/document/8327543. Acesso em: 29 de abril 2023.

FANNING, K.; CENTERS, D. P. Blockchain and its coming impact on financial services. *Journal of Corporate Accounting & Finance*, v. 27, n. 5, p. 53-57, 2016. Disponível em: https://onlinelibrary.wiley.com/doi/10.1002/jcaf.22179. Acesso em: 30 de abril 2023.

FARHADI, M.; ISMAIL, R.; FOOLADI, M. Information and communication technology use and economic growth. *PloS one*, v. 7, n. 11, p. e48903, 2012. Disponível em: https://www.researchgate.net/publication/233419400_Information_and_Communication_Technology_Use_and_Economic_Growth. Acesso em: 9 de maio 2023.

GLÄNZEL, W.; THIJS, B. Using 'core documents' for detecting and labelling new emerging topics. *Scientometrics*, v. 91, n. 2, p. 399-416, 2012. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.issi-society.org/proceedings/issi_2011/ISSI_2011_Proceedings_Vol1_26.pdf. Acesso em: 17 de junho 2023.

GOLDMAN, E. O.; ELIASON, L.C. *The Diffusion of Military Technology and Ideas*. Stanford University Press: Stanford, 2003. Disponível em: https://www.researchgate.net/publication/249909486_The_Diffusion_of_Military_Technology_and_Ideas_review. Acesso em: 17 de junho 2023.

GOMES, Julius *et al*. Cyber security business models in 5g. *A Comprehensive Guide to 5G Security*, p. 99-116, 2018. Disponível em: https://www.researchgate.net/publication/322466981_Cyber_Security_Business_Models_in_5G. Acesso em: 17 de junho 2023.

GRISSOM, A. The future of military innovation studies, *Journal of Strategic Studies*, 29 (5): 905–934, 2006. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/01402390600901067. Acesso em: 17 de junho 2023.

GUPTA, M.; DUBEY, A. E-commerce-study of privacy, trust and security from consumer's perspective. *transactions*, v. 37, p. 38, 2016. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ijcsmc.com/docs/papers/June2016/V5I6201647.pdf. Acesso em: 17 de junho 2023.

HOEHN, J. R.; SAYLER, K. M. National Security Implications of Fifth Generation (5G) Mobile Technologies. *Congressional Research Service (CRS) Reports and Issue Briefs*, 2021. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://crsreports.congress.gov/product/pdf/IF/IF11251/5. Acesso em: 13 de junho 2023.

JAMES, A. D. Emerging technologies and military capability. *Emerging critical technologies and security in the Asia-Pacific*, p. 6-21, 2016. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.files.ethz.ch/isn/174574/Policy%20Brief-Emerging%20Technologies%20and%20Military%20Capability.pdf. Acesso em: 13 de junho 2023.

KANIA, E. B.; VORNDICK, Wilson. Weaponizing Biotech: How China's Military Is Preparing for a 'New Domain of Warfare.'. *Defense one*, v. 14, 2019. Disponível em: https://www.defenseone.com/ideas/2019/08/chinas-military-pursuing-biotech/159167/. Acesso em: 19 de maio 2023.

KSHETRI, N. Can blockchain strengthen the internet of things?. *IT professional*, v. 19, n. 4, p. 68-72, 2017. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://libres.uncg.edu/ir/uncg/f/N_Kshetri_Can_2017.pdf. Acesso em: 19 de maio 2023.

LEE, In. The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model. *Internet of Things*, v. 7, p. 100078, 2019. Disponível em: https://www.researchgate.net/publication/278902692_Ecosystem_business_models_for_the_Internet_of_Things. Acesso em: 19 de maio 2023.

LEVY, S. *Hackers: heroes of the computer revolution*. Dell Publishing Co., 2001. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.temarium.com/wordpress/wp-content/uploads/downloads/2011/12/Levy_S-Hackers-Heroes-Computer-Revolution.pdf. Acesso em: 19 de maio 2023.

MALIK, V.; SINGH, S. Security risk management in IoT environment. *Journal of Discrete Mathematical Sciences and Cryptography*, v. 22, n. 4, p. 697-709, 2019. Disponível em: https://www.informahealthcare.com/doi/permissions/10.1080/09720529.2019.1642628?scroll=top. Acesso em: 19 de maio 2023.

MANDAL, Kumar; SINGHAL, Nikita; TYAGI, Deepak. Cybersecurity in the Era of Emerging Technology. In: KUMAR, Puneet *et al*. *Emerging Technology and Management Trends*. Delhi: Manglam Publications, 2023. Cap. 7. p. 98-124. Disponível em: ttps://www.researchgate.net/profile/Satish-Kumar-345/publication/372953153_Emerging_Technology_and_Management_Trends/links/64d0d129806a9e4e5cf6158c/Emerging-Technology-and-Management-Trends.pdf#page=108. Acesso em: 12 janeiro 2024.

MANDARINO JR, R. *Segurança e defesa do espaço cibernético brasileiro*. Recife: Cubzac, 2010.

MANZANO, J.; OLIVEIRA, J. *Algoritmos: lógica para desenvolvimento de programação de computadores*, 28 ed. São Paulo: ética, 2016. Disponível em: https://www.academia.edu/23834458/Algoritmos_Manzano. Acesso em: 30 de maio 2023.

MILLER, J., Green, I., Putland, G. *Emerging Technologies: A Framework for Thinking*. Australian Capital Territory Department of Education and Training, 2005. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.researchgate.net/profile/George_Veletsianos/publication/235939794_A_Definition_of_Emerging_Technologies_for_Education/links/550895120cf26ff55f8373a8/A-Definition-of-Emerging-Technologies-for-Education.pdf. Acesso em: 30 de maio 2023.

NSCAI, National Security Commission on Artificial Intelligence, *"First Quarter Recommendations"*, March 2020. Disponível em: https://www.nscai.gov/wp-content/uploads/2021/01/NSCAI-First-Quarter-Recommendations.pdf. Acesso em: 30 de maio 2023.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*, 2008. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://bitcoin.org/bitcoin.pdf. Acesso em: 30 de maio 2023.

NURSE, J.; CREESE, S.; DE ROURE, D. Security risk assessment in Internet of Things systems. *IT professional*, v. 19, n. 5, p. 20-26, 2017. Disponível em: https://www.researchgate.net/publication/318789039_Security_Risk_Assessment_in_Internet_of_Things_Systems. Acesso em: 5 de maio 2023.

O'NEILL, Maire *et al*. Insecurity by design: Today's IoT device security problem. *Engineering*, v. 2, n. 1, p. 48-49, 2016. Disponível em: https://www.researchgate.net/publication/301827951_Insecurity_by_Design_Today's_IoT_Device_Security_Problem. Acesso em: 5 de maio 2023.

OTAN. *Allied Joint Doctrine for Cyberspace Operations*. 2020. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf. Acesso em: 12 de jun. 2023.

OTAN. Emerging and disruptive technologies. *OTAN*, 2023. Disponível em: https://www.nato.int/cps/en/natohq/topics_184303.htm. Acesso em: 8 de jun. de 2023.

PANARELLO, Alfonso *et al*. Blockchain and IoT integration: A systematic survey. *Sensors*, v. 18, n. 8, p. 2575, 2018. Disponível em:

https://www.researchgate.net/publication/326868072_Blockchain_and_IoT_Integration_A_Systematic_Survey. Acesso em: 5 de maio 2023.

PATIL, P. Artificial intelligence in cybersecurity. *International journal of research in computer applications and robotics*, v. 4, n. 5, p. 1-5, 2016. Disponível em: https://www.academia.edu/25349174/ARTIFICIAL_INTELLIGENCE_IN_CYBER_SECURITY. Acesso em: 5 de maio 2023.

POHLE, J.; VOELSEN, D. Centrality and power. The struggle over the techno-political configuration of the Internet and the global digital order. *Policy & Internet*, v. 14, n. 1, p. 13-27, 2022. https://doi.org/10.1002/poi3.296. Disponível em: https://onlinelibrary.wiley.com/doi/10.1002/poi3.296. Acesso em: 10 de maio 2023.

POOLE, D. L.; MACKWORTH, A. K. *Artificial Intelligence: foundations of computational agents*. Cambridge University Press, 2010. https://doi.org/10.1017/9781108164085.

PORTELA, L. S. Geopolítica do espaço cibernético e o poder: o exercício da soberania por meio do controle. *Revista Brasileira de Estudos de Defesa*, v. 5, n. 1, 2018. Disponível em: https://rbed.abedef.org/rbed/article/view/75081. Acesso em: 1 de junho 2023.

RAJASEKAR, V.; PREMALATHA, J.; SARACEVIC, M. Cybersecurity in 5G and IoT Networks. *Secure Communication for 5G and IoT Networks*, p. 29-46, 2022. Disponível em: https://www.researchgate.net/publication/355726630_Cybersecurity_in_5G_and_IoT_Networks. Acesso em: 1 de junho 2023.

RID, Thomas. Cyber war will not take place. In: MAHNKEN, Thomas; MAIOLO, Joseph (ed.). *Strategic Studies: A Reader*. London: Routledge, 2014. p. 21. Disponível em: https://www.taylorfrancis.com/books/edit/10.4324/9781315814803/strategic-studies-thomas-mahnken-joseph-maiolo?refId=0f321b67-5e5f-4437-aa37-69adcdc9239f&context=ubx. Acesso em: 25 ago. 2023.

ROTOLO, D.; HICKS, D.; MARTIN, B. R. What is an emerging technology?. *Research policy*, v. 44, n. 10, p. 1827-1843, 2015. Disponível em: https://www.researchgate.net/publication/272164853_What_Is_an_Emerging_Technology. Acesso em: 1 de junho 2023.

SCHARRE, P. *Autonomous weapons and operational risk*. 2016. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Autonomous-weapons-operational-risk.pdf. Acesso em: 1 de junho 2023.

SCHARRE, P.; LAMBERTH, M. Artificial Intelligence and Arms Control. *arXiv preprint arXiv:2211.00065*, 2022. Disponível em: https://www.researchgate.net/publication/364987994_Artificial_Intelligence_and_Arms_Control. Acesso em: 1 de junho 2023.

SHA, Kewei *et al*. On security challenges and open issues in Internet of Things. *Future generation computer systems*, v. 83, p. 326-337, 2018. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0167739X17324883. Acesso em: 5 de junho 2023.

SHARMA, A.; JHA, R. K. A comprehensive survey on security issues in 5G wireless communication network using beamforming approach. *Wireless Personal Communications*, 2021. Disponível em: https://dl.acm.org/doi/abs/10.1007/s11277-021-08416-0. Acesso em: 5 de junho 2023.

SICARI, Sabrina *et al*. Security, privacy and trust in Internet of Things: The road ahead. *Computer networks*, v. 76, p. 146-164, 2015. Disponível em: https://www.researchgate.net/publication/270107935_Security_privacy_and_trust_in_Internet_of_Things_The_road_ahead. Acesso em: 5 de junho 2023.

SCHMITT, Olivier. Defence as War. In: GALBREATH, David J.; DENI, John R. (ed.). *ROUTLEDGE HANDBOOK OF DEFENCE STUDIES*. London: Routledge, 2018. Cap. 2. p. 18-28. Disponível em: https://www.routledge.com/Routledge-Handbook-of-Defence-Studies/Galbreath-Deni/p/book/9780367514532 . Acesso em: 5 de junho 202.

SRINIVASAN, R. Sources, characteristics and effects of emerging technologies: Research opportunities in innovation. *Industrial Marketing Management*, v. 37, n. 6, p. 633-640, 2008. Disponível em: https://www.researchgate.net/publication/222535627_Sources_Characteristics_and_Effects_of_Emerging_Technologies_Research_Opportunities_in_Innovation. Acesso em: 5 de junho 2023.

STIENNON, R. A short history of cyber warfare. In: GREEN, James A. (ed.). *Cyber Warfare: a multidisciplinary analysis*. [S.I]: Routledge, 2015. p. 7-33.

STOICA, Ion *et al*. A berkeley view of systems challenges for AI. *arXiv preprint arXiv:1712.05855*, 2017. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://sands.kaust.edu.sa/classes/CS290E/F19/papers/berkeley-sysai.pdf. Acesso em: 5 de junho 2023.

TEIXEIRA JÚNIOR, A. W. M.; LOPES, G. V.; FREITAS, M. T. D. As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica. *Carta Internacional*, *[S.*

l.J, v. 12, n. 3, p. 30–53, 2017. DOI: 10.21530/ci.v12n3.2017.620. Disponível em: https://www.cartainternacional.abri.org.br/Carta/article/view/620. Acesso em: 27 de junho 2023.

VALERIANO, B.; MANESS, R. C. *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press, USA, 2015. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://www.brandonvaleriano.com/uploads/8/1/7/3/81735138/cyber_war_versus_book_review_itp.pdf. Acesso em: 5 de junho 2023.

VERMA, S.; GUPTA, N. Application of Artificial Intelligence in Cybersecurity. *Innovations in Computer Science and Engineering: Proceedings of 7th ICICSE*, p. 65-72, 2020. Disponível em: https://www.researchgate.net/publication/339646771_Application_of_Artificial_Intelligence_in_Cybersecurity. Acesso em: 30 de junho 2023.

WORK, R. O.; BRIMLEY, S. Preparing for war in the robotic age. *Center for a New American Security*, Washington, DC, Tech. p. 28, 2014. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.files.ethz.ch/isn/176455/CNAS_20YY_WorkBrimley.pdf. Acesso em: 30 de junho 2023.

YAMPOLSKIY, R. V.; SPELLCHECKER, M. S. Artificial intelligence safety and cybersecurity: A timeline of AI failures. *arXiv preprint arXiv:1610.07997*, 2016. Disponível em: https://www.researchgate.net/publication/309424933_Artificial_Intelligence_Safety_and_Cybersecurity_a_Timeline_of_AI_Failures. Acesso em: 30 de junho 2023.

YEDUGONDLA, V. Implications of Emerging Technology on Cyber-Security. *Risk Group*, 2022. Disponível em: https://riskgroupllc.com/implications-of-emerging-technology-on-cyber-security/. Acesso em: 8 de jul. de 2023.

YLI-HUUMO, Jesse *et al*. Where is current research on blockchain technology?—a systematic review. *PloS one*, v. 11, n. 10, 2016. Disponível em: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477. Acesso em: 30 de junho 2023.

YOUSAF, Faqir *et al*. NFV and SDN—Key technology enablers for 5G networks. *IEEE Journal on Selected Areas in Communications*, v. 35, n. 11, p. 2468-2478, 2017. Disponível em: https://arxiv.org/abs/1806.07316. Acesso em: 30 de junho 2023.

Recebido em 28 de abril de 2024.
Aceito para publicação em 24 de junho de 2024.