FÁBIO LUIZ BENINCASA CORRÊA DOS SANTOS

COMO O DESENVOLVIMENTO DO METAVERSO PODE IMPACTAR A DEFESA NACIONAL?

Trabalho de Conclusão de Curso - Monografia - apresentada ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso de Altos Estudos de Política e Estratégia.

Orientador: Cel Refm João de Azevedo

Rio de Janeiro

2023

C2023ESG

Documento assinado digitalmente
gov.br
FABIO LUIZ BENINCASA CORREA DOS SANTOS
Data: 06/12/2023 19:45:11-0300
Verifique em https://validar.iti.gov.br

_____

FABIO LUIZ BENINCASA CORRÊA DOS SANTOS

Dados Internacionais de Catalogação na Publicação (CIP)

S237c Santos, Fabio Luiz Benincasa Corrêa dos

Como o desenvolvimento do metaverso pode impactar a Defesa Nacional? / CMG Fabio Luiz Benincasa Corrêa dos Santos. - Rio de Janeiro: ESG, 2023.

49 f.

Orientador: Cel. R/1 João de Azevedo

Trabalho de Conclusão de Curso - Monografia apresentada ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso de Altos Estudos de Política e Estratégia (CAEPE), 2023.

1. Segurança nacional – Brasil. 2. Soberania. 3. Brasil - Defesa. 4. Ambientes virtuais compartilhados. I. Título.

CDD - 330.981

Elaborada pelo bibliotecário Antonio Rocha Freire Milhomens – CRB-7/5917

A todos da turma CAEPE2023, pelo convívio cordial e fraterno.

Ao saudoso amigo Bezerril pela camaradagem e momentos de alegria, eternamente integrante da melhor turma.

A minha gratidão aos meus amados filho, filha e esposa, pela compreensão nos momentos de minhas ausências e omissões, em dedicação às atividades da Escola Superior de Guerra.

AGRADECIMENTOS

Aos meus professores de todas as épocas por terem sido responsáveis por parte considerável da minha formação e do meu aprendizado.

Ao meu Orientador, Cel Refm João de Azevedo, pelas importantes informações transmitidas, pela consideração e pela paciência nas correções.

Ao Corpo Permanente da ESG pelos ensinamentos e orientações que me fizeram refletir, cada vez mais, sobre a importância de se estudar o Brasil com a responsabilidade implícita de melhorá-lo.

Finalmente, aos estagiários da melhor Turma do CAEPE pela amizade e convívio harmonioso de todas as horas.

A ciência mais útil é aquela cujo fruto é o mais comunicável

Leonardo Da Vinci

RESUMO

Nesse trabalho o autor analisa como o metaverso pode impactar a Defesa Nacional, considerando que essa nova e disruptiva tecnologia irá ampliar ainda mais os horizontes do espaço cibernético. Fazendo uma analogia com a expansão do uso da internet e das redes sociais, as quais propiciaram o surgimento das ameaças cibernéticas e promoveram significativas mudanças culturais e comportamentais, depreende que o desenvolvimento do metaverso também causará grandes transformações na sociedade, potencializadas pela ubiquidade das informações digitais e pela reunião de outras emergentes e disruptivas tecnologias como a IoT, AI, VR, AR, *blockchain* e 5G em um novo ecossistema digital muito mais imersivo para os usuários. Devido à potencial capacidade do metaverso para criação de novas aplicações digitais e para influenciar os indivíduos, torna-se relevante a preocupação com a segurança das infraestruturas críticas, a preservação da integridade cultural e a manutenção da soberania. E tendo vista que as diversas organizações governamentais e instituições não poderão prescindir da utilização dos novos recursos tecnológicos inerentes ao metaverso, o autor faz uma avaliação sobre os riscos que podem surgir para a segurança e como mitigar as possíveis ameaças, a fim de fortalecer a Defesa Nacional.

Palavras-chave: segurança nacional – Brasil; soberania; Brasil – defesa; ambientes digitais compartilhados.

ABSTRACT

In this work, the author analyzes how the metaverse can impact National Defense, considering that this new and disruptive technology will further expand the horizons of cyberspace. Making an analogy with the expansion of the use of the internet and social networks, which led to the emergence of cyber threats and promoted significant cultural and behavioral changes, it can be seen that the development of the metaverse will also cause major transformations in society, enhanced by the ubiquity of digital information and by bringing together other emerging and disruptive technologies such as IoT, AI, VR, AR, blockchain and 5G into a new digital ecosystem that is much more immersive for users. Due to the potential capacity of the metaverse to create new digital applications and influence individuals, concerns about the security of critical infrastructures, the preservation of cultural integrity and the maintenance of sovereignty become relevant. And considering that the various government organizations and institutions will not be able to do without the use of new technological resources inherent to the metaverse, the author makes an assessment of the risks that may arise for security and how to mitigate possible threats, in order to strengthen Defense National.

Keywords*: national security – Brazil; Sovereignty; Brazil – defense; shared digital environments.*

SUMÁRIO

1 INTRODUÇÃO

Hoje observamos que está em curso uma significativa transformação no modo que a sociedade interage por meio das plataformas computacionais. Trata-se do advento do Metaverso, com todas as potenciais soluções, facilidades, recursos e oportunidades que essa nova e disruptiva tecnologia pode proporcionar. No entanto, se considerarmos o metaverso como uma nova dimensão do espaço cibernético, necessário se torna refletir sobre os seus possíveis impactos em áreas estratégicas do Estado, como a segurança e defesa.

Embora não se tenha ainda uma definição formal, o metaverso pode ser entendido como um ambiente digital persistente, desenvolvido por meio de modelagem em três dimensões (3D), que usa realidade virtual (VR), realidade aumentada (AR) e outras tecnologias avançadas para interação entre pessoas e com outros ativos, permitindo que os usuários tenham experiências pessoais e profissionais realistas *online*.

Alguns especialistas criticaram o recente uso do termo metaverso, que em suas opiniões corresponderia a algo que já existia, como os ambientes virtuais criados para simuladores e jogos de computador. Contudo, há estudos que demonstram que o metaverso é mais um exemplo das novas e disruptivas tecnologias, com potencial impacto à segurança global.

E o metaverso, por sua vez, é um ecossistema digital que irá concentrar as tecnologias mais avançadas, existentes e emergentes, como inteligência artificial (IA), internet das coisas (IoT), redes 5G, B5G e 6G, *blockchain*, *non-fungible tokens* (NFTs), criptomoedas e computação na nuvem. Isto faz com que o metaverso possa ser um dos principais recursos empregados no futuro, para diversos fins.

O metaverso, porém, é um tema com o qual muitas pessoas ainda não estão familiarizadas. Em geral, associa-se o metaverso à mera evolução das redes sociais, identificando-se inicialmente apenas suas aplicações comerciais e de entretenimento. Dessa forma, o debate acerca das possíveis ameaças presentes no metaverso é limitado.

Contudo, se tomarmos em conta as mudanças comportamentais e culturais ocorridas com o desenvolvimento da internet, com a popularização das mídias sociais e a ubiquidade das informações digitais, pode-se vislumbrar que algo muito mais profundo virá com o metaverso, que mudará radicalmente os hábitos, costumes e

regras da sociedade. Além disso, o uso desse novo e prolífico ambiente digital pelos diversos órgãos governamentais, incluindo as instituições voltadas à Defesa Nacional, implica em uma nova fonte de ameaças no espaço cibernético.

Esse processo de virtualização de ambientes, processos e sistemas no metaverso já está em curso. O uso dos “gêmeos digitais” no setor industrial e coorporativo é uma tendência que possibilita muitos ganhos em termos de agilidade, validação de informações, segurança na execução de testes, análises preditivas de resultados, receptividade do público, bem como redução do tempo gasto nessas atividades. Da mesma forma, organizações que lidam com dados sensíveis de indivíduos, infraestruturas críticas ou equipamentos militares também terão seus gêmeos digitais em algum ambiente virtual, o que abre a possibilidade de acesso não autorizado e a necessidade de proteção dessas informações.

Além disso, por ser um ambiente digital altamente imersivo, ameaças que usam a internet, como o terrorismo, desinformação, cooptação, *deepfakes*, além de outros crimes cibernéticos que impactam a Defesa Nacional, se tornarão mais intensas. No caso específico das Forças Armadas, seus militares terão consigo uma experiência de convívio virtual no metaverso, sem fronteiras ou correspondência fiel à realidade, trazida para dentro dos quartéis, que pode afetar o modo com que esses militares compreendam futuramente os princípios de hierarquia e disciplina.

É importante considerar nesse contexto que o fator humano é o principal ativo da segurança cibernética. A influência que o metaverso pode vir a exercer sobre os cidadãos representa um grande risco à segurança do ciberespaço e, por conseguinte, à integridade e segurança do Estado, uma vez que compromete o modo de vida da população e a sua integridade cultural.

Sendo assim, é importante acompanhar a evolução do metaverso, as possibilidades de emprego, possíveis vulnerabilidades e a sua regulação, de modo a antecipar a implementação de medidas de segurança visando a preservação dos interesses da Defesa Nacional.

1.1 Objetivo Final

Considerando o atual processo de desenvolvimento do metaverso e as decorrentes transformações que ocorrerão na sociedade em todo o mundo, o presente

trabalho visa identificar as futuras aplicações militares que as Forças Armadas poderão fazer uso do metaverso e as vulnerabilidades e ameaças na área da Defesa.

1.2 Objetivos Intermediários

De modo a proporcionar o silogismo necessário ao atingimento do objetivo final estabelecido nesse trabalho, serão considerados os seguintes objetivos intermediários:

a) contextualizar o conceito atual de metaverso;

b) identificar as perspectivas de desenvolvimento do metaverso;

c) identificar projetos atuais na área militar que utilizam o metaverso e as futuras possibilidades de emprego;

d) analisar vantagens e desvantagens do emprego militar do metaverso; e

e) identificar os possíveis impactos, como mudanças comportamentais da sociedade e influência de grandes corporações que possam provocar efeitos político-econômicos que afetem a Defesa Nacional.

1.3 Delimitação do Estudo

O trabalho pretende abordar especificamente os impactos do metaverso para o setor de Defesa Nacional, identificando especialmente as ameaças à segurança. Tendo em vista que em pouco tempo a utilização do metaverso será universal, com amplo acesso por pessoas de diversos países e a sua influência no âmbito das várias expressões do Poder Nacional, seja a econômica, científico-tecnológica, psicossocial e até mesmo política, o que tornaria a pesquisa muito abrangente, o enfoque do trabalho será para a expressão militar da Defesa Nacional.

Embora haja boas perspectivas para as aplicações militares do metaverso, sendo inevitável a expansão do seu uso no âmbito das Forças Armadas, o trabalho será direcionado às vulnerabilidades contidas no metaverso e as possíveis ameaças à segurança.

Esse corte também é necessário para evitar um espectro de pesquisa demasiadamente amplo, considerando ainda que as aplicações benignas do metaverso na área militar poderão ser criteriosamente incorporadas e que o desafio

maior é identificar e antecipar-se às vulnerabilidades que o metaverso pode trazer à Defesa Nacional.

1.4 Relevância e Justificativa do Estudo

O metaverso é uma tecnologia em processo de desenvolvimento, recentemente anunciada como uma grande tendência para o futuro. O surgimento de novos ambientes digitais aumenta o espectro do espaço cibernético, de modo que é importante acompanhar os estudos que têm sido feitos acerca das implicações do metaverso para o setor de defesa.

De acordo com a atual Política Nacional de Defesa, o espaço cibernético brasileiro requer grande atenção quanto à sua segurança e defesa, uma vez que é essencial para garantir o funcionamento dos sistemas de informações, de gerenciamento e de comunicações de interesse nacional (BRASIL, 2020b).

A importância dessa atenção reflete-se na Ação Estratégica de Defesa (AED) nº 11 da Estratégia Nacional de Defesa: “incrementar as capacidades de defender e de explorar o espaço cibernético” (BRASIL, 2020b).

Dessa forma, por ser um tema ainda recente e que se relaciona com os campos de conhecimento da Defesa e Segurança, especialmente numa área de grande interesse estratégico que é a defesa cibernética, considera-se que o assunto possui relevância para estudos da Escola Superior de Guerra.

1.5 Hipóteses

Não foram identificadas hipóteses para o presente trabalho.

2 REFERENCIAL TEÓRICO

O referencial teórico advém de material já publicado sobre o tema, especialmente artigos científicos que servem como embasamento às informações contidas nesse trabalho.

Foram selecionados artigos que abordam o advento do metaverso, tecnologias aplicadas, implicações futuras e, também, artigos acerca das transformações ocorridas com o surgimento da internet e das redes sociais, de modo a possibilitar uma analogia quanto às mudanças que podem advir com o desenvolvimento do metaverso.

Nesse sentido, iniciando uma análise sobre ameaças cibernéticas relacionadas às redes sociais, encontra-se o artigo de Johnson (2013), que trata da defesa cibernética de infraestruturas críticas, onde cita alguns papéis desempenhados pelas redes sociais, tanto para motivar indivíduos a participarem da execução de ataques, que podem ser do tipo negação de serviço, quanto na ocultação da origem desses ataques. Segundo Johnson, devido a arquitetura das redes sociais, é difícil identificar se um ataque cibernético foi ou não patrocinado por um estado, ao passo em que afirma que os governos fazem uso do recrutamento de redes criminosas antissociais para lançar ataques a infraestruturas críticas de terceiros.

Thompson (2012) aborda o uso de ferramentas de mídia social por indivíduos e organizações com intuito de radicalizar outros indivíduos para a mudança política e social, o qual se tornou cada vez mais popular à medida que a internet penetra mais no mundo e os dispositivos de computação móvel são mais acessíveis. Esclarece ainda por que os aplicativos de mídia social tem sido a plataforma perfeita para dar voz ao extremismo e analisa o uso das mídias sociais e sua influência na radicalização das populações no Norte da África e no Oriente Médio durante o ano de 2011.

Observando que a facilidade de uso e a conectividade fornecidas pelas mídias sociais tem ocasionado um conflito crescente entre as necessidades pessoais dos usuários militares e a segurança operacional militar, Dressler, Bronk e Wallach (2015) apresentam um estudo realizado a partir da coleta de informações que militares postam em suas redes sociais. Com base nos dados abertos coletados, aplicando técnicas de aprendizado de máquina, foi possível identificar potenciais alvos de ações de inteligência, indicando uma possível vulnerabilidade para o Departamento de Defesa dos EUA e os efeitos negativos da obtenção de dados pessoais de militares.

Especificamente sobre o metaverso e as ameaças à segurança, Metz e Gurău (2022) descrevem o metaverso como exemplo de tecnologia emergente e disruptiva, com grande impacto para a segurança global. Fazem ainda uma análise das implicações socioeconômicas no meio civil e das ameaças assimétricas, como o terrorismo. Relatam ainda os impactos das aplicações militares do metaverso, as oportunidades inerentes, os riscos e desafios, mesmo considerando a ainda insipiente versão atual do metaverso.

Aini et al. (2022) buscam examinar o papel da Defesa Nacional da Indonésia para se contrapor às ameaças que o metaverso representa à segurança do ciberespaço e aos cidadãos indonésios, destacando o fator humano como principal ativo da segurança cibernética, além da necessidade de se preservar o modo de vida da população, a integridade cultural e a segurança do Estado.

Quanto à privacidade no metaverso, Nair, Garrido e Song (2022) destacam os riscos que os ambientes virtuais representam para obtenção de dados pessoais de usuários. Por meio de um experimento, consistindo em um jogo em realidade virtual com trinta pessoas, demonstram que um programa invasor é capaz de extrair diversas informações biométricas como altura e envergadura, e demográficas como idade e sexo de todos os participantes, em poucos minutos, o que denota um risco à privacidade sem precedentes.

A respeito de possíveis aplicações militares do metaverso, Fawkes e Cheshire (2022) investigam as origens e as últimas ideias sobre o metaverso, considerando a criação de um “Military Metaverse CONOPS”. O CONOPS (Conceito de Operações) descreve um futuro ecossistema de modelagem e simulação de defesa (M&S) construído em tecnologias, padrões e abordagens de metaverso, juntamente com benefícios, casos de uso e ações a serem tomadas, explicando por que e como as tecnologias podem ser reunidas para benefício da defesa.

Farrkhodovna e Alisher qizi (2022) exploram o conceito de soberania dos países no ciberespaço. Enquanto a soberania territorial pode ser facilmente reconhecida pelas fronteiras territoriais, a soberania cibernética de um país envolve uma abordagem mais complexa. Fazem um estudo com base no exemplo da República Popular da China, examinando suas rígidas práticas de regulação da internet e suas consequências, que podem incluir novos processos de governança no metaverso.

Cabe ressaltar que a relevância dos estudos acerca do desenvolvimento do metaverso se alinham com o contido na Política Nacional de Defesa, na Estratégia Nacional de Defesa e no Livro Branco de Defesa Nacional (BRASIL, 2020a, 2020b) quanto à importância da Defesa Cibernética.

2.1 Metodologia

Para esse trabalho, pretende-se obter os dados necessários prioritariamente em artigos científicos que abordam a temática dos impactos do metaverso na segurança global, identificando aquilo que potencialmente pode representar ameaça à nossa Defesa Nacional.

No entanto, considera-se também relevante pesquisar artigos que tratam sobre o desenvolvimento do metaverso, de modo que se possa descrever os fatores que levam à sua veloz ascensão como um novo ambiente digital e à ampliação das suas possibilidades de emprego.

A pesquisa será por meio de fontes divulgadas na internet, que sejam confiáveis e de acesso livre. De modo a preservar a segurança e evitar a exposição de vulnerabilidades, será evitada a solicitação formal de informações às organizações militares dedicadas à defesa cibernética.

Dessa forma, o trabalho pode ser desenvolvido a partir de informações de caráter ostensivo, de material já publicado, disponíveis em repositórios na internet reconhecidos, cujo conteúdo será concatenado pelo autor, de modo a estabelecer uma linha de raciocínio que leve à resposta do problema de pesquisa proposto.

A classificação da pesquisa, quanto aos meios de investigação, corresponde à pesquisa bibliográfica, a qual segundo Fachin (2017), é a base para as demais. Ruiz (2006) explica que a pesquisa bibliográfica consiste no exame e análise do que já se produziu sobre determinado tema. Para Marconi e Lakatos (2010), a pesquisa bibliográfica refere-se àquela que se realiza a partir de material disponível, decorrente de pesquisas anteriores, em documentos impressos, como livros, periódicos, artigos e outros. Quanto aos fins, na classificação de Vergara (2016), considera-se como aplicada. Segundo Vergara (2016), a pesquisa aplicada tem como finalidade a prática e é motivada por uma necessidade imediata ou não.

3 COMO O USO DO METAVERSO SE TORNARÁ INTENSO E UNIVERSAL

Podemos considerar que o metaverso ainda está em uma fase embrionária do seu desenvolvimento. No entanto, há perspectiva para um crescimento acelerado da utilização dos universos digitais nos próximos anos. Nesse capítulo serão abordados alguns dos fatores que poderão alavancar o crescimento do metaverso, iniciando por uma breve contextualização do que é essa nova tecnologia.

3.1 Contextualização: o que é o Metaverso?

Atribui-se o surgimento do termo “metaverso” ao romance de ficção científica *Snow Crash* (Avalanche), do escritor Neal Stephenson, lançado em 1992. Nessa icônica obra, o protagonista Hiro transita sua personalidade entre um entregador de pizzas na realidade e um hacker samurai no metaverso, um mundo digital onde cada indivíduo vive através de seu avatar uma outra vida completamente diferente da verdadeira (STEPHENSON, 2015). A etimologia do termo metaverso indica que a palavra deriva pela junção do prefixo meta, do grego “metá”, que indica “além de”, e da palavra universo; do inglês “metaverse”, usado por Neal Stephenson.

O termo metaverso ganhou força quando em 2021 Mark Zuckerberg anunciou em um evento do Facebook que a empresa passaria a estar sob uma nova marca denominada Meta, visando explorar o novo conceito que é o metaverso (META, 2021). Após esse anúncio, a empresa Meta sofreu elevadas perdas financeiras, além de queda dos valores de suas ações. Contudo, o CEO Mark Zuckerberg mantém firme o projeto de investir nessa área, considerada promissora (HERN, 2022).

De fato, o desenvolvimento do metaverso ainda está numa fase inicial. Pagliusi (2023), em palestra realizada no Clube Naval, ressaltou que o metaverso alcançará seu amadurecimento a partir de 2030. Sobre esse novo conceito, Pagliusi destacou a importância do *blockchain* como amálgama desse novo espaço virtual, para a validação das informações e segurança das transações realizadas no metaverso.

Assim, o conceito de metaverso remete a um ambiente digital imersivo e interativo, cujo desenvolvimento se tornará viável com a incorporação de novas tecnologias e maior capacidade computacional, com potencial de transformar o modo

de vida da sociedade, mas com oportunidades e ameaças que ainda precisam ser estudadas.

3.2 Fatores que favorecem a evolução do Metaverso

Pode-se inferir o desenvolvimento do metaverso por meio de uma breve analogia com a evolução da própria internet. Quando no final da década de 1990 houve a grande popularização da internet, foi por meio da preexistente rede de telefonia fixa que os usuários comuns se conectavam. De fato, como concluído por Leiner et al. (1999), tecnologias anteriores como o telégrafo, o telefone e o rádio favoreceram a evolução da internet. De modo semelhante, a evolução do metaverso será impulsionada tanto pela própria internet, a qual já compreende novas e disruptivas tecnologias digitais, quanto pelo desenvolvimento em diversas outras áreas científicas, como a óptica, confecção de malhas, tecidos e materiais para sensores e o aprimoramento de baterias elétricas, sendo muitas dessas inovações com aplicação em IoT.

Também por analogia com a evolução da internet, o metaverso possui um grande fator impulsionador, que é o seu potencial para oferecer conteúdo adulto. Hughes (2000) cita como a indústria pornográfica tanto promoveu o desenvolvimento quanto estimulou a adoção de novas tecnologias digitais. Assim como o comércio de conteúdo erótico promoveu a popularização dos aparelhos de videocassete, na internet levou ao desenvolvimento e disseminação de tecnologias como privacidade das transações eletrônicas para cartões de crédito, estratégias de anúncios *online* e, especialmente, a criação de novos formatos de vídeo, que possibilitaram o advento de grandes plataformas de *streaming*, como Youtube e Netflix (PAASONEN, 2015).

É relevante considerar esse fato, pois uma das ameaças que podem ser potencializadas pelo metaverso são o assédio e abuso sexual nos ambientes digitais, que normalmente tem como principais vítimas mulheres e crianças.

A pandemia de COVID-19, que foi uma emergência sanitária a nível global, constituiu um grande catalisador do uso de novas tecnologias digitais. Conforme avaliação da Organização para a Cooperação e Desenvolvimento Econômico - OCDE (*Organisation for Economic Co-operation and Development* - OECD), a COVID-19 fez com que vários países acelerassem seu processo de transformação digital. Com a pandemia, crianças passaram a assistir às aulas remotamente; funcionários passaram

a trabalhar em casa, em sistema de *home office*; e muitas empresas adotaram modelos de negócios digitais para manterem suas operações e preservar fluxos de receitas. Enquanto isso, foram desenvolvidas novas aplicações móveis para rastrear a evolução da pandemia e pesquisadores passaram a empregar inteligência artificial para aprender mais sobre o vírus e acelerar a busca por uma vacina. O tráfego da internet em alguns países aumentou até 60% logo após o surto, sublinhando a aceleração digital que a pandemia desencadeou (OECD, 2020).

Bill Gates, co-fundador da Microsoft, assinala em seu livro "*How to Prevent the Next Pandemic*" como a pandemia da COVID-19 acelerou o processo de digitalização na sociedade. Cita que alternativas digitais antes consideradas inferiores passaram a ser preferenciais, exemplificando que "um vendedor oferecer apresentar seu produto por uma videoconferência passou a ser algo aceitável" Gates (2022). Com o isolamento, as pessoas tiveram que recorrer às ferramentas digitais existentes, como compras de supermercado *online* e videoconferência e usá-las de forma diferente e criativa, como por exemplo a realização de festas de aniversário virtuais.

No mesmo livro, Gates (2022) cita como o metaverso, ao simular a presença física nos ambientes e com o uso de tecnologia de áudio espacial, pode suplantar as atuais restrições das videoconferências, especialmente no que se refere à percepção da comunicação não verbal. E apresenta sua perspectiva sobre o metaverso:

> Estamos nos aproximando de um limite em que a tecnologia começa a replicar verdadeiramente a experiência de estar no escritório. As mudanças que vimos no local de trabalho são precursoras de mudanças que penso que veremos em muitas áreas. Estamos caminhando em direção a um futuro onde todos passaremos mais tempo nos espaços digitais. O metaverso pode parecer um conceito novo agora, mas à medida que a tecnologia melhorar, ele evoluirá para o que parece mais uma extensão do nosso mundo físico.

A eclosão de uma nova pandemia certamente iria acelerar o uso do metaverso. Mas não será necessário que isso ocorra para que, em pouco tempo, o metaverso torne-se cada vez mais familiar e presente na vida das pessoas. À medida que o desenvolvimento tecnológico possibilite maior capacidade computacional a nível mundial e maiores velocidades de transmissão de dados, as aplicações no metaverso vão se tornar mais tangíveis para a sociedade.

3.3 As novas tecnologias usadas no metaverso

Cabe destacar o conceito de *digital twins*, ou “gêmeos digitais”, que é a digitalização em 3D de uma estrutura física existente no mundo real. Em relação aos ambientes de simulação que conhecemos hoje, a tecnologia de gêmeo digital é muito mais interativa.

Tanto os gêmeos digitais como as atuais simulações por computador são baseadas em modelos virtuais, mas existem algumas diferenças relevantes. Um gêmeo digital é de fato um ambiente virtual, o que o torna consideravelmente mais apto a fornecer dados. A diferença entre gêmeo digital e simulação é basicamente uma questão de escala. Uma simulação em geral estuda um processo específico. Pode ser um teste de esforço de material, ensaio de um componente ou cálculo de uma trajetória. Já o gêmeo digital pode executar uma grande quantidade de simulações simultâneas, o que permite analisar vários processos.

No metaverso, a inteligência artificial terá um papel fundamental, especialmente por permitir a criação de personagens com os quais poderemos interagir de diversas formas. A individualidade de cada usuário, tanto pessoas quanto organizações, poderá ser assegurada por meio de *blockchain*, assim como todas as transações no ambiente digital. A propriedade de ativos virtuais é implementada por meio de NFTs.

A interação no metaverso, em ambientes de VR ou AR, ocorrerá com o desenvolvimento de dispositivos de IoT, como óculos de realidade virtual, luvas hápticas e trajes capazes de transmitir a sensação de tato aos usuários, além se sensores biométricos que possibilitarão a digitalização do estado dos usuários no mundo digital.

Verificamos, porém, que após o anúncio do Facebook de novos investimentos voltados para o metaverso e da mudança do seu nome comercial para “Meta”, ocorreu uma queda do valor dos seus ativos no mercado financeiro, acompanhada de críticas e ceticismo quanto a viabilidade do metaverso. Isso porque, de fato, não há hoje uma infraestrutura computacional capaz de processar todos os dados de modo a manter o ambiente virtual disponível e funcional para bilhões de usuários, em nível global.

No entanto, esse vem sendo o desafio constante da internet, desenvolver cada vez mais capacidade de processamento e maiores velocidades de resposta. Assim, é de se esperar que ao longo dos anos a evolução tecnológica permita que

gradualmente o ambiente virtual do metaverso seja construído, havendo estimativas de que, a partir de 2030, o metaverso já faça parte da nossa vida.

4 PERSPECTIVAS PARA USO DO METAVERSO

Embora o metaverso ainda esteja num período inicial de desenvolvimento, podemos constatar muitas aplicações empregadas hoje em dia que certamente estarão integradas ao metaverso no futuro. É o caso das maquetes digitais em 3D de prédios e construções e dos simuladores de treinamento.

Segundo Chandar (2022), em previsão divulgada pela empresa de serviços financeiros Morgan Stanley, o metaverso poderá movimentar cerca de US$ 112 bilhões em 2030. Dessa forma, a sociedade está cada vez mais atenta às oportunidades no metaverso, o que leva ao desenvolvimento de novas aplicações que gerem receitas nesse novo ambiente digital.

4.1 As aplicações do metaverso

Sem entrar no contexto dos jogos, diversas aplicações atuais convergem para um futuro uso do metaverso. Destacam-se as aplicações que são desenvolvidas com o conceito de gêmeos digitais. Aplicações que usam gêmeos digitais estão presentes nos setores de equipamentos de geração de energia, como motores e turbinas; estruturas como edifícios, plataformas e seus sistemas; operações de manufatura; serviços de saúde e atendimento médico; indústria automotiva e planejamento urbano (IBM, 2023b).

Especificamente na área militar, o emprego de simuladores para treinamentos táticos ou de emergências já é bastante difundido. No entanto, com a possibilidade de implementação de gêmeos digitais, essas aplicações tornar-se-ão ainda mais aprimoradas.

Nesse contexto, segundo Metz e Gurău (2022), a evolução do metaverso tem grandes implicações no setor militar, especialmente quanto à segurança, ao multiplicar as oportunidades existentes e revelar novas, assim como os riscos, vulnerabilidades e ameaças. No entanto, treinamentos que de outra forma seriam muito perigosos, impossíveis, contraproducentes e/ou caros, no metaverso podem ser executados. Por exemplo, pode-se realizar adestramentos de minagem e desminagem de terrenos, instalação de explosivos em infraestruturas críticas e qualificar em menor tempo os militares em novas habilitações operacionais. No metaverso, novas armas e equipamentos poderiam ser testados em simulações para

avaliação operacional. Além disso, o metaverso pode vir a se tornar tanto uma fonte para recrutamento de pessoal como também um meio de retenção de talentos.

De acordo com análise do Fórum Econômico Mundial (*World Economic Forum* - WEF), o metaverso deve desenvolver-se inicialmente no setor industrial. Aliás, o uso dos gêmeos digitais na indústria já vem dando bons resultados em termos de produtividade e eficiência. Embora atualmente o uso dos gêmeos digitais esteja voltado ao monitoramento e análise de processos, o potencial do metaverso industrial é muito maior. De acordo com o WEF, à medida que a capacidade de processamento, velocidade de transmissão de dados e novas tecnologias de detecção, interface e AI forem incorporadas, “será possível passarmos de um estado de consciência para um estado de controle” (BATRA, 2023).

Segundo o Fórum, em vez de apenas monitorar digitalmente o chão de fábrica, será possível manipulá-lo virtualmente. Trabalhadores poderão realizar manutenção de equipamentos utilizando diagramas detalhados e instruções visuais passo a passo projetadas em seu campo de visão. Eventualmente, alguns desses trabalhadores poderão efetuar manutenções na segurança de suas mesas, assumindo o controle virtual de robôs de reparo, os quais poderão comandar remotamente. Os robôs automatizados operarão em realidades físicas e digitais, ganhando a consciência de cada pessoa, máquina e processo no chão de fábrica para que possam orquestrar as suas tarefas da forma mais eficiente.

Para o Fórum, o que se chamaria de “metaverso do consumidor” se desenvolverá posteriormente. E terá o proveito das várias tecnologias que forem evoluindo no âmbito do setor industrial, as quais vão desde a microóptica e interfaces táteis avançadas até a percepção de detecção de AI. Na perspectiva do Fórum Econômico Mundial, “em vez de gastarmos energia na prossecução de um metaverso de consumo ainda embrionário, devemos concentrar a nossa visão no metaverso diretamente à nossa frente, o qual está firmemente enraizado nos locais onde trabalhamos” (BATRA, 2023).

4.2 O metaverso no mundo atual

Conforme relembra Baughman (2022), “o metaverso é uma tecnologia emergente e, portanto, é difícil avaliar o impacto que terá na sociedade, na política, na economia, nas normas internacionais, na segurança nacional e na sociedade como

um todo". Baughman analisa como a China está se posicionando para liderar e, potencialmente, dominar o desenvolvimento do metaverso, com o objetivo declarado de alcançar o "patamar mais elevado da inovação", com investimento e apoio de algumas das suas maiores empresas de tecnologia, bem como do próprio Partido Comunista Chinês.

Segundo Baughman, a própria estratégia de segurança do ciberespaço do Partido Comunista Chinês ressalta a importância da soberania, da construção de normas internacionais, do desenvolvimento da economia digital e da expansão da cultura da China. E para alcançar estes objetivos estratégicos no ciberespaço, a China acredita que precisa ser pioneira na tecnologia do metaverso para poder moldar o futuro da Internet.

Baughman descreve que como líder no desenvolvimento do metaverso, a China poderá, no campo econômico, obter vantagens em face da sua economia digital em ascensão e, no campo político, colocar-se em posição de moldar as normas internacionais relativas ao metaverso, além de fortalecer o seu *softpower* por meio da difusão da sua cultura nesse novo canal.

A China especialmente possui avançadas iniciativas para o metaverso. Um exemplo é o projeto anunciado para a cidade de Xangai, que inclui o metaverso em sua estratégia de desenvolvimento. As metas digitais incluem a construção de redes 5G e de banda larga mais rápidas, a construção de fábricas inteligentes e hospitais digitalizados, o desenvolvimento de IA e serviços baseados em dados e o reforço de aplicações para idosos e pessoas com deficiência (WEI, 2022).

Assim como Xangai, o governo municipal de Seul, capital da Coreia do Sul, anunciou um plano de ação de cinco anos para construir um grande gêmeo digital da cidade, como um canal alternativo para fornecer acesso aos serviços municipais aos cidadãos, englobando serviços administrativos relativos à economia, cultura, turismo, educação e reclamações civis (SEOUL, 2021).

Como exemplos de possíveis aplicações do metaverso no setor de defesa, Hyun (2022) descreve que a KAI (*Korea Aerospace Industries*) desenvolveu um sistema que materializa as aeronaves ou satélites (aviões de combate, helicópteros, satélites, drones etc.) em tamanho real 3D quando o usuário acessa o espaço cibernético usando óculos VR e luvas VR. O sistema permite não apenas ver, mas também tocar diretamente a imagem virtual através de luvas virtuais.

Hyun cita ainda que a empresa sul coreana Hancom Frontis divulgou ao público o treinamento de voo de um caça da Força Aérea e de um helicóptero de ataque Apache do Exército, com simulação de exercícios de tiro tático. Segundo Hyun, tal demonstração “convergiu tecnologias como metajogo, tecnologia tátil virtual (háptica), *Big Data*, 5G etc. para o treinamento de manobra de tropas e exercício de funções de Comando em cada nível e para o Estado-Maior da operação”. Relata ainda que o Exército da Coreia do Sul está desenvolvendo uma plataforma *online* baseada em jogos para implementar o exercício militar em VR de forma realista.

No caso particular da China, é necessário que se tenha atenção para o fato de um país que possui um regime governamental autoritário e que impõe restrições às liberdades individuais da sua sociedade vir a controlar as tecnologias e plataformas digitais empregadas no metaverso, em função da influência que pode ser exercida nos campos político, econômico e psicossocial dos Estados menos desenvolvidos, o que pode enfraquecer a sua soberania.

4.3 Uso do metaverso no Brasil

Conforme anunciado pela PETROBRAS (2022), foi assinado em 04/OUT/2022, o contrato com a empresa Seatrium (antiga Sembcorp Marine), de Singapura, para construção da plataforma P-82. Prevista para ser a décima plataforma a ser instalada no Campo de Búzios (maior campo em águas profundas do mundo), no pré-sal da Bacia de Santos, a plataforma será uma das maiores a operar na indústria de petróleo e gás mundial e está programada para entrar em operação em 2026.

A P-82 terá diversas tecnologias de ponta. Porém, destaca-se no seu projeto a utilização da tecnologia de gêmeos digitais, para viabilizar simulações e testes remotos, antes da entrada da plataforma em operação, visando garantir a sua segurança e a confiabilidade operacional.

Especialistas acreditam que o uso de sistemas de gêmeos digitais nos setores portuário e marítimo possui grande potencial de se desenvolver nos próximos anos. A avaliação é que os “digital twins” podem trazer benefícios às áreas de produção e de operação (DIGITAL twin..., 2022).

Na Marinha do Brasil, a construção das quatro novas Fragatas Classe “Tamandaré”, pelo consórcio Águas Azuis, composto pelas empresas ThyssenKrupp

(Alemanha), Embraer e Atech (Brasil) e gerenciado pela Emgepron, utilizará tecnologias de gêmeos digitais e realidade aumentada na sua execução. A primeira fragata está programada para entrega em 2025 e, partir de então, cada ano terá a entrega de uma nova embarcação, até 2028. Todo projeto de construção está sendo realizado de forma digital, sem uso de manuais ou desenhos técnicos em papel (*paperless*).

As atividades de construção da primeira fragata já iniciaram, na Thyssenkrupp Estaleiro Brasil Sul, em Itajaí-SC. Com o apoio da matriz da Thyssenkrupp na Alemanha, foram implementados mais de 20 totens com computadores na área de produção. Nesses equipamentos, os profissionais envolvidos no projeto conseguem acessar os sistemas, desenhos no formato 2D e 3D, *check-lists*, procedimentos e manuais, tudo sempre atualizado em tempo real pelo time de engenharia do Brasil e da Alemanha. A digitalização da construção dos navios por meio de gêmeos digitais permite a aceleração de processos diários, como o apontamento de mão de obra, solicitação interna de consumíveis, rastreabilidade de chapas, perfis, tubulações e controle da qualidade (ALVES, 2023).

A existência de dados sensíveis sobre ativos estratégicos para o país, sejam plataformas de exploração de petróleo, infraestrutura portuária e até mesmo meios das Forças Armadas, em tão alto grau de detalhamento, em plataformas digitais que em muitos casos são pertencentes a empresas estrangeiras, pode vir a constituir no futuro uma grande vulnerabilidade para atos hostis. Dessa forma, a garantia da segurança das informações nesses projetos é de grande interesse da Defesa Nacional.

5 IMPACTOS DO ADVENTO DO METAVERSO PARA A DEFESA NACIONAL

Para analisar os possíveis impactos do metaverso, é importante estar atento à forma como as novas e relevantes tecnologias estão sendo desenvolvidas e utilizadas, para que se possam identificar oportunidades e, ao mesmo tempo, conduzir análises de risco para verificar os potenciais danos. Para isso, pode-se considerar as oportunidades e ameaças hoje existentes na internet e adicionar a elas os recursos estendidos que o metaverso oferece. A utilização de uma análise anterior das oportunidades e ameaças da internet nos fornece um ponto de partida de lições aprendidas e não requer que se inicie um estudo partindo do zero (MARLER, ABDURAHAMAN, *et al.*, 2023).

5.1 Considerações sobre o advento da internet

O dia 1º de julho de 1988 é citado pela *National Science Foundation* (NSF) dos EUA como “o dia em que o mundo mudou”. Essa data marca a conclusão da atualização das redes e *backbone* da NSFNET (*National Science Foundation Network*), que entrou em operação em 1980 e vinha sofrendo com o crescimento exponencial do tráfego nas redes após a sua abertura para conexão de Universidades, órgãos governamentais e comerciais, em 1986 (NATIONAL SCIENCE FOUNDATION, 2008).

O ano de 1995, em especial, constitui um grande marco na história da internet. Foi nesse ano que o consórcio W3C (*World-Wide Web Consortium*) consolidou-se na coordenação e controle da *World-Wide Web*. Também em 1995, uma resolução *do Federal Networking Council* (FNC) dos EUA ratificou o termo “internet” como referente ao sistema global de informações baseado no protocolo TCP/IP (LEINER, CERF, *et al.*, 1999).

Com o crescimento acelerado do número de usuários comerciais e com os provedores de rede privados tornando-se capazes de absorver esse tráfego, a NSF anunciou em 1995 a retirada do financiamento governamental à operação da NSFNET e o descomissionamento dos seus servidores, fato que marcou a privatização da internet (NATIONAL SCIENCE FOUNDATION, 2003).

Um novo desafio passou a existir para a Defesa Nacional a partir desses eventos: a ameaça cibernética. Nota-se que o termo “*cyber*” passou a constar na NSS

(*National Security Strategy* - Estratégia de Segurança Nacional) dos EUA a partir de 1998, referindo-se a ameaças como *cyber-crime* e *cyber-attack* (UNITED STATES, 1998).

No Brasil, a menção à possíveis ataques cibernéticos surge na Política de Defesa Nacional do ano de 2005 (BRASIL, 2005). Mas isso não implica que a defesa cibernética já não constasse, mesmo de forma implícita, nos documentos de defesa de alto nível anteriores. Diante disso, quando as ameaças advindas do metaverso passarão a constar de forma explícita nas estratégias de defesa? Considerando o impacto do avanço da internet na defesa cibernética, o metaverso poderá analogamente tornar-se uma nova ameaça nos próximos anos.

5.2 Considerações sobre o advento das redes sociais

Com o avanço da internet, surgem as redes sociais, as quais atualmente conectam pessoas e organizações com amigos, familiares, clientes e indivíduos que possuem interesses em comum. Com o desenvolvimento do metaverso, como será a interação em redes sociais num ambiente digital muito mais imersivo? Analisando o impacto que as redes sociais trouxeram para a Defesa Nacional, podemos vislumbrar os possíveis efeitos do metaverso.

Além de conectar pessoas, as redes sociais tornaram-se também veículos de mídia, capazes de propagar notícias rapidamente. Passaram a ter grande relevância econômica e valor estratégico, em face das informações que armazenam sobre seus usuários. Tal fato gera diversos conflitos de interesse, em nível internacional, como o que tem sido vivenciado entre a China e alguns países do ocidente.

Um exemplo disso é o caso do aplicativo para celulares “Tik Tok”, que é uma rede social de compartilhamento de vídeos, de origem chinesa. Conforme noticiado pela Rede Globo de Televisão, o Reino Unido decidiu em16 de março de 2023 banir o aplicativo *Tik Tok* dos celulares de trabalho dos funcionários do governo. A reportagem destaca que a decisão em Londres seguiu o posicionamento de Canadá, Bélgica, Comissão Europeia e EUA. Esses países do ocidente alegam que dados dos usuários do *Tik Tok* podem acabar nas mãos do governo da China (REINO Unido..., 2023).

Segundo a reportagem da TV Globo, desde 2020 o governo dos EUA tem ameaçado banir o uso do aplicativo no país, tendo como proposta para sua

continuidade que os donos chineses do *Tik Tok* vendam suas participações para empresas norte-americanas. Destaca ainda o alcance do aplicativo, com mais de 1,5 bilhões de usuários, sendo que muitos também usam o aplicativo como fonte de renda.

No ponto de vista dos governos, o *Tik Tok* é uma brecha na segurança nacional, pois as informações capturadas dos usuários alimentam modelos matemáticos de AI, capazes de prever o comportamento de uma população, o que poderia abalar democracias e até mesmo interferir no resultado de eleições (TV GLOBO, 2023).

Esse é mais um capítulo que mistura economia e segurança nacional na disputa entre China e EUA, que mostra como podem ser os conflitos também no metaverso.

Thompson (2012) ao analisar a onda de protestos ocorrida no Norte da África e no Oriente Médio em 2011, que ficou conhecida como “Primavera Árabe”, cita como fatos em comum nesses eventos: a ausência de um líder oficial na organização dos protestos e a influência que os meios de comunicação social parecem ter exercido na intensidade da manifestação.

Thompson explica ainda como a mídia social conecta facilmente as pessoas com um público amplo. A sinergia cria um movimento em massa de pessoas com ideias semelhantes. Dessa forma, as redes sociais ajudam a formar o que podemos chamar de “comunidades” na internet.

Um fato importante que Thompson destaca é que cada pessoa com um telefone celular e um aplicativo de mídia social é um sensor capaz de coletar e distribuir dados de inteligência bruta em tempo real. Cita como exemplo o fato de canais de notícias terem aproveitado essa capacidade durante alguns anos, quando os telefones celulares com câmeras foram lançados no mercado e os usuários contribuíram com seus vídeos para os noticiários noturnos.

Especificamente sobre os protestos de 2011 no Egito, Thompson descreve que os influenciadores e blogueiros nas redes sociais examinaram dados sobre a densidade de conexões sociais (quantas pessoas estão conectadas na região?), a densidade de informação (de quantas fontes a informação está sendo compartilhada?) e a densidade das percepções emocionais (os leitores estão vivenciando o evento como se eles próprios estivessem lá?). Afirma Thompson que, se houver uma alta densidade de conexões, se a informação estiver sendo transmitida através de múltiplas fontes e as pessoas se sentirem conectadas ao evento como se o

estivessem vivendo, então há uma maior probabilidade de radicalização, pois as pessoas se sentirão inclinadas a envolverem-se em vez de ficarem à margem vendo as coisas acontecerem.

Segundo Thompson, os meios de comunicação social efetivamente conectam as pessoas a diferentes fontes de informação e trazem o indivíduo para o evento, para que ele ou ela possa vê-lo desenrolar-se à medida que acontece. Isto aumenta uma reação emocional dentro do indivíduo para se tornar um apoiador envolvido e radical. Da mesma forma que os governos e os políticos utilizam as redes sociais para espalhar a sua influência, comunicar com os apoiantes e angariar fundos, os grupos radicais podem utilizar as redes sociais para os mesmos fins. O exemplo de Thompson leva a inferir que o grau de influência que poderá ser exercido por meio do metaverso e suas redes pode ser ainda maior.

5.3 Ameaças do metaverso no campo militar

Dressler (2015) por sua vez, estuda especificamente a utilização das redes sociais por militares norte-americanos. Assim como muitas pessoas, os militares também podem vir a expor informações sensíveis na internet, sejam elas dados operacionais ou de sua vida pessoal. Apesar da implementação de políticas de segurança pelo Departamento de Defesa dos EUA, o risco ainda existe. De fato, a internet e as redes sociais transformaram-se em um ambiente operacional rápido e adaptável, que proporciona uma vantagem significativa em termos de custo-benefício em relação às técnicas tradicionais de seleção de alvos. Por meio da exploração de dados disponíveis nas redes *Facebook* e *Linkedin*, Dressler demonstrou como é possível que agentes adversos selecionem alvos entre os militares para exercerem influência.

Analogamente, se considerarmos o uso particular do metaverso por militares no futuro, uma exploração de dados como atualmente pode ser feita nas redes sociais poderá revelar informações muito mais consistentes para agentes adversos que buscam selecionar alvos militares cooptáveis.

Cabe destacar o experimento citado Nair, Garrido e Song (2022), em que numa plataforma virtual de jogo, foi possível coletar diversos dados biométricos dos participantes. Essas informações, correlaciodas às demais referências sobre cada

indivíduo, alimentam a base de dados no metaverso com dados que podem revelar muito mais sobre os usuários.

No metaverso, onde a variedade de dados sobre cada indivíduo é ainda maior, conforme demonstrado por Nair, Garrido e Song, os riscos de comprometimento de informações e de acesso a dados de militares são grandes, o que certamente poderá trazer impactos à segurança.

Vanorio (2022), em texto sob égide da *NATO Defense College Foundation* (Fundação do Colégio de Defesa da Organização do Tratado do Atlântico Norte - OTAN) conta que a Meta (antiga Facebook) adquiriu recentemente a *startup* de dados sintéticos AI.Reverie e a consolidou em sua divisão de Laboratórios de Realidade, a qual é dedicada à construção de um mundo virtual compartilhado. A empresa AI.Reverie havia sido contratada pela Força Aérea dos EUA (USAF), para desenvolver um sistema baseado em IA para gestão de conflitos e melhoria sistemas de comando e controle. O contrato de serviços de três anos, no valor de US$ 950 milhões, foi rescindido “por conveniência”, em correspondência com a aquisição da AI.Reverie pela Meta. Mesmo com o término dessa relação com o Pentágono, o conhecimento capitalizado pela AI.Reverie certamente acelerará as capacidades da Meta em produzir dados sintéticos para treinar algoritmos de aprendizagem de máquina para construir tipos de metaversos que manterão uma dualidade civil-militar latente.

Descreve ainda que, em 2020, a AI.Reverie celebrou acordos para melhorar a coleta de informações do Exército e da Força Aérea dos EUA, bem como para melhorar as capacidades de navegação em terrenos difíceis, utilizando dados sintéticos para treino. Especificamente, o produto da AI.Reverie apoiaria a 7ª Ala de Bombas, parte da unidade de comando da USAF que conduz operações de dissuasão nuclear e de ataque global (Comando de Ataque Global, 8ª Força Aérea).

Esse relato indica o risco que existe de que organizações privadas, ou até mesmo estrangeiras, possam ter acesso a dados das Forças Armadas, referentes aos seus sistemas no metaverso. Dada a possibilidade de agentes adversos, por meio do metaverso, explorarem um grande leque de informações, como padrões de comportamento e dados biométricos, as informações sensíveis acerca de dados operacionais e de técnicas empregadas em treinamento ficam ao alcance desses agentes adversos, que terão a vantagem de conhecer as capacidades das Forças.

O desafio da soberania no ciberespaço fica evidente nos dias de hoje ao verificar as dificuldades para rastrear os crimes cibernéticos. A China por exemplo é

um país de tem dedicado significativos investimentos para o desenvolvimento do metaverso, buscando estar à frente nessa nova tecnologia (BAUGHMAN, 2022). Tal corrida tecnológica por parte dos países mais avançados pode constituir uma ameaça à soberania dos demais estados, o que indica a necessidade de se construir normas internacionais sobre esse tema.

Descreve Baughman que essa mesma mentalidade de estar à frente está sendo aplicada pelos militares chineses para construir um “metaverso militar”, o qual chama de “battleverse”, visando aprimorar a capacidade do Exército da Libertação Popular da China em educação, treinamento, testes, pesquisa e comunicações de apoio que possam proporcionar vantagens militares significativas. Melhor formação, pesquisa e educação podem conduzir a uma força de combate mais eficaz e letal.

Baughman sugere ainda que podem surgir conflitos à medida que o metaverso é implementado e utilizado como a internet, considerando que os setores de tecnologia da informação já tem sido identificados como infraestruturas críticas, e que o metaverso fará parte disso quando estiver operacional. Sobre essa possibilidade, Baughman afirma:

> Talvez, o metaverso se torne tão transparente que os limites entre a internet e a realidade se tornem confusos. À medida que a sociedade, incluindo os militares, depende do metaverso nas operações diárias, haverá maiores riscos e potenciais consequências na perturbação ou destruição do metaverso. [...] Devem ser criadas normas para evitar possíveis conflitos, mas o próprio ecossistema também deve tornar-se resiliente à medida que o metaverso se torna um alvo valioso na guerra.

Assim como nas Forças Armadas as suas redes de dados e infraestrutura de TI atualmente constituem um importante ativo a ser protegido no contexto da cibersegurança, no futuro as aplicações que as Forças venham a desenvolver no metaverso poderão, de forma análoga, tornarem-se alvos críticos, de modo que a própria segurança da infraestrutura do metaverso será importante ativo para a Defesa Nacional.

5.4 Considerações sobre Segurança e Defesa

Um aspecto importante que pode impactar a segurança no metaverso é a questão da soberania no ciberespaço. Farrkhodovna e Alisher qizi (2022) destacam que ao contrário da soberania territorial, em que há um controle quanto à jurisdição, uma vez que os estados têm suas fronteiras estabelecidas, no ciberespaço não há uma jurisdição digital e que as normas internacionais não têm acompanhado a evolução digital. Não há normas internacionais que abordem explicitamente a segurança no metaverso.

Farrkhodovna e Alisher qizi mostram o exemplo da China como um estado que busca estabelecer suas fronteiras digitais, ao adotar um sistema rígido de controle e restrição do uso da internet, denominado “Golden Shield” (Escudo Dourado), o qual foi introduzido para regular as relações jurídicas na esfera da internet. Esse sistema impõe censura e restrições ao anonimato, além de banir domínios da *web* e serviços considerados desnecessários.

No entanto, segundo Farrkhodovna e Alisher qizi, embora tal sistema possa ser eficaz em termos de redução da criminalidade e para garantia da soberania no ciberespaço, há o risco de tornar o ambiente político no país mais frágil, ao inibir a competitividade na arena política, o que no futuro poderia levar a uma crise política.

Johnson (2013) destaca o uso das redes sociais na realização de diversos ataques cibernéticos, citando exemplos do ocorrido na Estônia em 2007, Bielorrússia, Lituânia e Geórgia em 2008 e Paquistão e Índia em 2010. Segundo Johnson, a infraestrutura computacional das redes sociais dificulta determinar se ataques cibernéticos teriam sido orquestrados por estados ou não. Contudo, Johnson revela que as redes sociais foram usadas para motivar indivíduos a participarem em ataques de negação de serviço (*Deny of Service* - DoS) em massa, disseminar informações e fornecer acesso a recursos desenvolvidos por grupos cibercriminosos para ataques cibernéticos.

No contexto da Segurança Nacional, Marler (2023) analisa as oportunidades e ameaças do metaverso para o Departamento de Segurança Interna dos EUA (*U.S. Department of Homeland Security* - DHS) e ressalta que o metaverso de fato tem relevância para o DHS. No artigo divulgado pela Rand Corporation, identifica as seguintes oportunidades e ameaças:

a) Oportunidades:

– Inteligência e investigação - o metaverso permite monitorar possíveis ameaças e coletar provas que ajudem a garantir proteção. As informações digitais do metaverso podem ajudar a prevenir ataques criminosos no mundo real e também a investigá-los posteriormente;

– Divulgação e disseminação de informação - permitir ao governo comunicar-se com a população sobre uma variedade de questões de segurança. O metaverso poderia ser usado para promover campanhas, divulgar programas interativos e de sensibilização sobre questões afetas à segurança;

– Preparo e prontidão - o material usado atualmente sobre a preparação para catástrofes naturais, como terramotos e tsunamis, por exemplo, utiliza principalmente texto e imagens estáticas para comunicar os perigos desses fenômenos e encorajar as pessoas a manterem abastecimento adequado de alimentos não perecíveis e água potável, bem como bolsa de suprimentos e outros itens de sobrevivência. Uma simulação de preparação baseada no metaverso permitiria que as pessoas vivenciassem um terremoto simulado e vissem os danos que ele pode causar, bem como examinassem o conteúdo de uma bolsa de suprimentos. As pessoas poderiam participar de exercícios de evacuação de suas casas ou bairros, bem como de locais públicos, com a maioria dos outros evacuados sendo simulados. Isso permitiria aos usuários ganhar experiência com evacuação sem a necessidade de coordenação massiva. Princípios semelhantes podem ser aplicados em toda variedade de situações de interesse. Em geral, ambientes virtuais e simulações podem reduzir riscos de lesões, reduzir custos, facilitar repetições e permitir revisões pós-ação mais eficazes e objetivas; e

– Treinamento - os ambientes virtuais podem ser úteis para agentes de segurança no treinamento para atuar em eventos catastróficos, incluindo ataques terroristas e desastres naturais. A realização de exercícios em grande escala pode ser extremamente dispendiosa, exigindo a coordenação e transporte de grande número de pessoas e muitas vezes o fechamento temporário do local envolvido. O treinamento em um metaverso poderia evitar esses problemas, permitindo que um determinado número de pessoas treine em um ambiente realisticamente lotado, no qual a maioria das pessoas são operadas como simulações de computador. Poderá haver um grande custo inicial para o governo criar os gêmeos digitais para preparação e treinamento, mas poderá haver um bom retorno desse investimento, especialmente se estes ativos

puderem ser multiuso. Por exemplo, o mesmo estádio virtual poderia ser usado para planejamento de eventos, exercícios de segurança, trabalhos de manutenção e publicidade.

b) Ameaças:

– Desinformação - no metaverso as narrativas podem ser disseminadas por meio de dimensões multissensoriais, talvez atuando mais poderosamente nos facilitadores psicológicos, como o viés de confirmação, que constroem credibilidade em informações falsas. O metaverso também traz a possibilidade de *deepfakes* multissensoriais, que poderiam imitar líderes governamentais ou outros, a fim de semear ideias nocivas destinadas a desestabilizar as instituições e polarizar o público. Tal como ocorre nas redes sociais atualmente, campanhas de desinformação deliberada podem buscar atingir pessoas carentes e comunidades marginalizadas para fomentar a desconfiança nas instituições governamentais, agora de numa forma diferente, por exemplo, como um avatar altamente realista representando o que poderia ser um líder ou decisor político. Além disso, com a ampla disseminação de desinformação, os usuários podem até ver o metaverso como totalmente falso, onde nada é confiável, incluindo informações importantes que o governo procura divulgar (por exemplo, avisos relacionados com a aproximação de um furacão ou outro desastre). Uma complexidade adicional da desinformação no metaverso é que grande parte do conteúdo pode ser passageiro e efêmero - mais semelhante a conversas presenciais informais do que aos dados, que são permanentemente armazenados em conteúdos algorítmicos que um público amplo pode observar. Como resultado, pode ser mais difícil para o governo e até mesmo para as próprias plataformas do metaverso rastrearem a propagação de informações falsas e enganosas e identificar os principais criadores e disseminadores desse conteúdo. Este desafio analítico também poderia tornar mais difícil para o governo agir contra a desinformação em campanhas coordenadas por estados estrangeiros. Até mesmo entender o escopo do desafio da desinformação pode ser um problema, sendo necessário que o governo considere cuidadosamente como monitorar a atividade no metaverso de modo a garantir que possa compreender os desafios e, ao mesmo tempo, proteger as liberdades civis e a privacidade.

– Abuso e assédio - o combate à exploração infantil pode ser afetado por novas formas de assédio e abuso que poderão ocorrer no metaverso. A Internet já permitiu novas formas de abuso sexual e outros, especialmente contra as mulheres e

crianças e existe o risco de que as plataformas do metaverso possam permitir ainda mais a exploração infantil, o abuso sexual e o tráfico sexual. Uma experiência social mais envolvente também poderia expandir o potencial para esquemas de confiança, como fraudes e golpes que tendem a atacar os idosos e outras pessoas que são novas na tecnologia ou que são socialmente vulneráveis. Será importante que seja desenvolvido um engajamento eficaz e seguro para compreender as formas de abuso que podem ocorrer no metaverso. O governo terá que estar preparado para o caso de vítimas apresentarem novos tipos de danos que poderão não ter equivalente no mundo físico. Os efeitos que o abuso e o assédio sofridos no metaverso podem ter sobre os resultados no mundo físico são pouco estudados. Há estudos que sugerem que o elevado senso de realidade que os usuários vivenciam no metaverso significa que as experiências adversas no metaverso terão maiores impactos psicológicos do que as mesmas experiências no mundo real (VRIES, 2011). No entanto, outros podem argumentar que o metaverso fornece espaço para a saída construtiva de comportamentos que seriam considerados incontestavelmente abusivos no mundo físico;

– Violência Organizada - o metaverso poderia fornecer um novo local para atos de terrorismo ou de violência organizada. Assim como acontece com as plataformas de redes sociais existentes, o metaverso pode se tornar um fórum para radicalizar pessoas, recrutar terroristas, permitir às organizações planejarem e coordenarem ataques e incitarem ataques violentos generalizados. Também poderá proporcionar ambientes poderosos de planejamento e treinamento para ataques terroristas e outros ataques criminosos organizados. Os próprios ataques podem ocorrer em metaversos, o que pode afetar o bem-estar das pessoas ou até mesmo evoluir para violência no mundo real. Além disso, o metaverso poderia ajudar várias organizações terroristas a recrutarem novos membros. O governo terá que estar preparado para interagir com comunidades virtuais emergentes e garantir que possa lidar com estes tipos de ameaças de uma forma que reflita o seu papel legítimo na proteção das liberdades civis.

– Cibersegurança - o metaverso pode tornar-se uma linha de frente para vários tipos de crimes cibernéticos e fraudes ao consumidor que expandem as formas existentes desses crimes na internet. Além disso, o surgimento de metaversos como ambientes persistentes, nos quais as pessoas possuem bens que podem ser adquiridos com dinheiro real (provavelmente com base em tecnologia *blockchain*) e

usado em vários ambientes, tem o potencial de criar uma nova classe de crimes contra a propriedade. A investigação de tais crimes provavelmente exigirá um conjunto de habilidades diferente do trabalho policial tradicional ou da segurança cibernética praticada atualmente. Uma questão adicional de segurança cibernética para a qual o governo terá de estar preparado é a possibilidade de que governos estaduais, locais, tribais e territoriais ou proprietários e operadores de infraestruturas críticas possam eles próprios utilizar metaversos para prestação de serviços ou treinamentos de vários tipos. Se os governos e os provedores de infraestruturas críticas se tornarem mais dependentes dos metaversos para treinamento ou outras atividades, poderão surgir novos vetores de ataques maliciosos. Será necessário estar preparado para os desafios de segurança cibernética que surjam nessas aplicações do metaverso e, potencialmente, fornecer orientação sobre as melhores práticas ou mesmo resposta a incidentes cibernéticos no metaverso.

– Questões de ética e igualdade - os desafios concernentes a ética e igualdade podem estar presentes em muitas ameaças. Tais desafios demandam a necessidade de preparo, monitoramento e resposta aos efeitos potencialmente prejudiciais para o Estado decorrentes do metaverso. No entanto, o próprio governo deverá estar atento aos seus valores éticos fundamentais para que as suas respostas a estes desafios não impliquem por si só em violação de liberdades civis e outros direitos, haja vista o possível uso de ferramentas analíticas e de vigilância. Para mitigar esse risco é necessário construir uma relação de confiança e de apoio das partes interessadas, como a iniciativa privada, membros do Congresso e organizações da sociedade civil. A consulta das partes interessadas será importante para garantir que se possa desenvolver e alavancar parcerias para rastrear ameaças e responder de forma mais eficaz. O envolvimento com estes grupos também pode garantir que as comunidades marginalizadas possam expressar as suas preocupações sobre a desinformação, o abuso, a desigualdade entre outras ameaças que possam surgir.

Dessa forma, Marler (2023) indica que para que o Departamento de Segurança Interna dos EUA possa lidar com as oportunidades e ameaças do metaverso, é importante fazer uma análise a partir das experiências já obtidas com o advento da internet, otimizar suas próprias capacidades e estabelecer relações de confiança e cooperação com demais setores envolvidos e partes interessadas. Ao considerar esses três grandes esforços, o DHS poderia colaborar com proprietários e

operadores de infraestruturas críticas e governos e, assim, fornecer melhor orientação ou suporte apropriado nas questões afetas ao metaverso.

Rosenberg (2023) alerta que as tecnologias de mídia interativa em tempo real podem no metaverso ser combinadas com tecnologias interativas de AI. Por exemplo, agentes conversacionais poderão ser configurados com sistemas de controle de *feedback*, que transmitem influência e monitoram as reações do usuário em tempo real, otimizando assim seu impacto persuasivo.

As técnicas poderão incluir o uso de porta-vozes virtuais que parecem, soam e agem como outros usuários humanos e são projetados para facilitar aos usuários-alvo uma conversa amigável, que os manipule em direção à agenda de influência de patrocinadores terceirizados, que poderão ser desde agentes corporativos até atores estatais. Segundo Rosenberg, isso poderia "impactar significativamente a liberdade cognitiva e a agência epistêmica dos usuários-alvo, o que não é apenas um risco para os consumidores individuais, mas um amplo perigo social que pode impactar a própria democracia" (ROSENBERG, 2023).

Por estas razões, Rosenberg sugere que legisladores devem considerar propor regulamentações rígidas que protejam as populações do abuso ou uso indevido de tecnologias de mídia interativa, especialmente aquelas que "fechem o ciclo" sobre os usuários em tempo real e estabeleçam sistemas de controle de *feedback* alimentados por AI, que transmitam persuasão, coerção ou manipulação. Além disso, sugere que os reguladores poderiam proibir a apropriação das características faciais, qualidades vocais ou padrões de fala de um usuário para implantar em agentes conversacionais e poderiam exigir que todos os agentes virtuais parecessem, soassem ou se comportassem de uma maneira que os identificasse como material promocional interativo.

5.5 Ameaças à Defesa Nacional no Brasil

Para a Defesa Nacional, considerando os possíveis impactos no campo da Expressão Militar do Poder Nacional, é importante acompanhar a evolução dos acontecimentos concernentes ao desenvolvimento do metaverso, de modo que se possa mitigar os riscos no futuro.

As Forças Armadas dependem dos recursos computacionais para se manterem atualizadas em relação à evolução das condições operacionais e

economicamente sustentáveis. Dessa forma, a parceria com demais organizações, sejam elas públicas ou privadas, civis ou militares, é necessária para o desenvolvimento de novas aplicações para as Forças, como sistemas corporativos e ambientes digitais de treinamento.

O uso do metaverso pelas Forças Armadas, especialmente em função das tecnologias de AR, VR e gêmeos digitais para treinamento de militares ou avaliação operacional de novos meios e armamentos, gera oportunidades para que agentes adversos possam efetuar exploração de informações, as quais em geral estão na nuvem, armazenadas em servidores de terceiros, em localização geográfica nem sempre conhecida.

Eventos transformadores que ocorreram em outros países, podem futuramente vir a se desenvolverem também no Brasil. A exemplo do que foi observado na “Primavera Árabe”, que teve as redes sociais como indutores de grandes movimentos populares, no metaverso as discussões político-sociais podem ser ainda mais intensas. Isso poderá acarretar manifestações populares de magnitude sem precedentes. Situações de extrema polarização política podem agravar ainda mais os riscos que esses protestos poderão representar à ordem e a estabilidade das Instituições, o que afeta também a Defesa Nacional.

As características mais interativas e imersivas do metaverso, aliadas ao crescente uso dos ambientes digitais pelas novas gerações, tende a fazer com que as “comunidades” virtuais de pessoas com interesses comuns criem vínculos ainda mais fortes. Tais comunidades poderão ter militares entre seus participantes. No caso das Forças Armadas brasileiras, que têm como pilares fundamentais a hierarquia e a disciplina, a quebra desses princípios pode trazer riscos à integridade das Forças, caso a lealdade dos militares mude de lado.

Como ocorre com as redes sociais, o metaverso poderá ser tornar um meio para que agentes adversos possam buscar militares alvo para exercer influência. Além disso, o metaverso gera condições nas quais os militares podem vivenciar conflitos de interesses entre a sua realidade virtual e a vida real nas organizações militares. Esses conflitos podem causar desde problemas disciplinares até a cooptação de militares por agentes adversos para diversos atos, como espionagem, vazamento de dados, sabotagem, roubo de armas e até mesmo ações terroristas.

Tendo em conta o fato do metaverso estar se desenvolvendo gradualmente no setor industrial, notadamente em função da incorporação da tecnologia de gêmeos

digitais (BATRA, 2023), é de se esperar que os sistemas de controle de infraestruturas críticas também passem a adotar as facilidades que o metaverso pode proporcionar. Sistemas de distribuição de água, energia elétrica, instalações portuárias e outros terão o seu gêmeo digital no metaverso para redução de custos operacionais, o que pode aumentar a vulnerabilidade dessas infraestruturas à ataques de agentes adversos.

O rápido desenvolvimento tecnológico e a migração de atividades e serviços para o metaverso, como o que já podemos notar com a difusão das aplicações de inteligência artificial, acarretará significativas transformações no mercado de trabalho que podem aumentar o nível de desemprego, causando impactos sociais negativos e insegurança. Dessa forma, é necessário que o governo e a sociedade acompanhem adequadamente as mudanças de modo a identificar e aproveitar as oportunidades de novos tipos de emprego e ocupações que poderão ser gerados ao longo do período de transição tecnológica, adotando políticas públicas para capacitação de profissionais para o uso das novas tecnologias.

Dada a ubiquidade das informações digitais, o desenvolvimento de novos mundos virtuais, sem fronteiras e com ilimitada capacidade de interação, requer especial atenção para os aspectos relacionados à segurança, visando o bem-estar da sociedade e evitar os impactos negativos à Defesa Nacional.

Dessa forma, o desenvolvimento do metaverso torna necessário que sejam elaboradas políticas públicas que garantam o uso seguro dessa nova tecnologia, por indivíduos e instituições, bem como a construção de normas internacionais acerca do tema. Os documentos de Defesa de alto nível, coma PND e a END, também devem conter ações visando preservar a segurança e a soberania do Estado em face da evolução do metaverso, atualizando-se a um mundo em rápida transformação.

6 CONCLUSÃO

O metaverso consistirá em um ambiente virtual muito mais imersivo e interativo do que as plataformas digitais que conhecemos hoje. O que torna o metaverso diferente das experiências que a internet atualmente proporciona é a incorporação de novas e disruptivas tecnologias que darão suporte a esse novo mundo digital. Embora ainda esteja numa fase inicial de desenvolvimento, estima-se que a partir de 2030 o metaverso passe a fazer parte das nossas vidas.

De forma análoga ao ocorrido com a expansão da internet, verifica-se que o metaverso tem o potencial de evoluir e tornar-se uma tecnologia universalmente utilizada. As possibilidades de interação e transmissão de informações são enormes e o processo de transformação digital, que teve grande impulso em decorrência da pandemia da COVID-19, é um dos fatores que contribuem para o amplo uso do metaverso na sociedade.

A utilização dos gêmeos digitais no setor industrial tem apresentado vantagens como maior eficiência e produtividade e representa um processo inicial de desenvolvimento do metaverso. Da mesma forma, o controle de infraestruturas críticas também poderá ser realizado por meio de gêmeos digitais no futuro, o pode representar uma vulnerabilidade para ataques cibernéticos através do metaverso.

Também com base nas transformações que já vivenciamos com o advento da internet, que trouxe consigo a ameaça cibernética, e do crescimento das redes sociais, que têm capacidade de influenciar significativas mudanças comportamentais na sociedade, verifica-se por analogia que o metaverso poderá trazer novos riscos, com potencial de causar impactos à Defesa Nacional.

Ameaças como o terrorismo, desinformação e crimes cibernéticos serão muito mais intensas no metaverso. Embora o poder militar possa fazer um uso benéfico do metaverso, especialmente para ambientes de treinamento, planejamento militar e avaliação operacional de meios, com significativa economia de recursos, suas informações sensíveis poderão ser alvo de agentes adversos, assim como os próprios militares, que estarão mais expostos à influência e cooptação.

Assim, quanto ao pessoal militar, é importante considerar que o metaverso será um ambiente digital capaz de absorver um grande leque de informações sobre os usuários, por meio do qual agentes adversos poderão realizar ações de exploração para identificar possíveis militares-alvo para exercerem influência.

Além disso, as mudanças comportamentais e o relacionamento mais intenso em comunidades virtuais podem levar militares a conflitos de interesse que afetam os pilares de hierarquia e disciplina, o que representa um sério risco à integridade das instituições militares, mediante atos que podem consistir desde problemas disciplinares a ações influenciadas por agentes adversos como espionagem, vazamento de dados, sabotagem, roubo de armas e até mesmo atos terroristas.

Considerando os atuais desafios hoje existentes quanto à soberania no ciberespaço, a corrida dos países tecnologicamente mais desenvolvidos pela supremacia digital, especialmente por um país de regime governamental autoritário como a China, representará uma grande ameaça aos Estados menos desenvolvidos, nos campos político, psicossocial e econômico, enfraquecendo a sua soberania.

Será necessário que o governo e a sociedade acompanhem adequadamente as mudanças no mercado de trabalho em função da migração de atividades e serviços para o metaverso e da implementação de novas tecnologias, de modo a identificar e aproveitar as oportunidades de novos tipos de empregos e ocupações que poderão ser gerados ao longo do período de transição tecnológica, adotando políticas públicas para capacitação de profissionais para o uso das novas tecnologias, evitando assim os impactos sociais negativos e insegurança devido ao desemprego.

Dada a ubiquidade das informações digitais, o desenvolvimento de novos mundos virtuais, sem fronteiras e com ilimitada capacidade de interação, requer especial atenção para os aspectos de segurança, visando o bem-estar da sociedade e evitar os impactos negativos à Defesa Nacional.

Dessa forma, o desenvolvimento do metaverso requer que sejam elaboradas políticas públicas atualizadas que garantam o uso seguro dessa nova tecnologia, por indivíduos e instituições, bem como a construção de normas internacionais sobre o metaverso. Os documentos de defesa de alto nível, coma a PND e a END, também devem conter ações visando preservar a segurança e a soberania do Estado brasileiro em face do desenvolvimento do metaverso, adequando-se a um mundo em rápida transformação.

REFERÊNCIAS

AINI, Ameilia *et al.* Indonesian State Defense as an effort to counter the cyberspac esecurity threat of metaverse. **International Journal of Arts and Social Science**, Jember, ago. 2022. 17 - 24. Disponível em: https://www.ijassjournal.com/2022/V5I8/414665868.pdf. Acesso em: 27 ago. 2023.

ALVES, Soraia. Tecnologias como gêmeos digitais e realidade aumentada ajudam Marinha a construir navios militares. **Época Negócios**, 24 jan. 2023. Disponível em: https://epocanegocios.globo.com/futuro-da-industria/noticia/2023/01/tecnologias-como-gemeos-digitais-e-realidade-aumentada-ajudam-marinha-a-construir-navios-militares.ghtml. Acesso em: 6 ago. 2023.

AVATAR. *In*: MERRIAM Webster Dictionary, 25 set. 2023. Disponível em: https://www.merriam-webster.com/dictionary/avatar. Acesso em: 27 set. 2023.

BATRA, Nishant. The metaverse will make its biggest impact on industry. Here's why. **Word Economic Forum**, 13 Jan. 2023. Disponível em: https://www.weforum.org/agenda/2023/01/metaverse-biggest-impact-industry-davos2023. Acesso em: 6 ago. 2023.

BAUGHMAN, Josh. Enter the Battleverse: China's Metaverse War. **Military Cyber Affairs**, Tampa, 05, May 2022. Disponível em: https://digitalcommons.usf.edu/mca/vol5/iss1/2. Acesso em: 26 ago. 2023.

BRASIL. **Decreto nº 5.484, de 30 de junho de 2005.** Aprova a Política de Defesa Nacional, e dá outras providências. Brasília, DF: Presidência da República, 2005. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/decreto/d5484.htm. Acesso em: 27 ago. 2023.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional**. Brasília, DF: MD, 2020a. Versão sob apreciação do Congresso Nacional (Lei Complementar 97/1999, art. 9º, § 3º). Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/livro_branco_congresso_nacional.pdf. Acesso em: 31 mar. 2023.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa. Estratégia Nacional de Defesa**. Brasília, DF: MD, 2020b. Versão sob apreciação do Congresso Nacional (Lei Complementar 97/1999, art. 9º, § 3º). Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf. Acesso em: 31 mar. 2021.

CHANDAR, Vijay. Investing in the metaverse: new opportunities in virtual worlds. **Morgan Stanley**, New York, 15 Dec. 2022. Disponível em: https://www.morganstanley.com/articles/metaverse-opportunities-virtual-reality-augmented-reality-technologies. Acesso em: 6 ago. 2023.

DIGITAL twin ampliará eficiência operacional no setor portuario preveem especialistas. **Portos e Navios**, 3 nov. 2022. Disponível em: https://www.portosenavios.com.br/noticias/portos-e-logistica/digital-twin-ampliara-eficiencia-operacional-no-setor-portuario-preveem-especialistas. Acesso em: 6 ago. 2023.

DRESSLER, Judson ; BRONK, Christopher; WALLACH, Daniel S. Exploiting military opsec through open-source. **IEEE Military Communications Conference**, Tampa, 26 Oct. 2015. Disponível em: https://ieeexplore.ieee.org/abstract/document/7357484. Acesso em: 7 jun. 2023.

ERICSSON. **Discover the power of 5G**. Stockholm: Ericsson, 2023a. Disponível em: https://www.ericsson.com/en/5g. Acesso em: 30 mar. 2023.

ERICSSON. **What is 6G?** Stockholm: Ericsson, 2023b. Disponível em: https://www.ericsson.com/en/6g. Acesso em: 30 mar 2023.

FACHIN, Odília. **Fundamentos de Metodologia**. 6. ed. São Paulo: Saraiva, 2017.

FARRKHODOVNA, Inoyatova O.; ALISHER QIZI, Aminova A. Cybersovereignty: The Example of China. **Texas Journal of Multidisciplinary Studies**, Plano, v. 14, p. 119-124, 2022. Disponível em: https://zienjournals.com/index.php/tjm/article/view/2843. Acesso em: 30 mar. 2023.

FAWKES, Andrew J.; CHESHIRE, Nick. **Military Metaverse CONOPS**. [*S. l.*]: NATO; S & T Organization, 2022. Disponível em:

https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-MSG-197/MP-MSG-197-26.pdf. Acesso em: 31 mar. 2023.

GATES, Bill. **How to prevent the next pandemic**. New York: Canadiana, 2022.

HERN, Alex. Facebook owner Meta to sack 11,000 workers after revenue collapse. **The Guardian**, 09 Nov. 2022. Disponível em: https://www.theguardian.com/technology/2022/nov/09/mark-zuckerberg-meta-to-sack-11000-workers-after-revenue-collapse-facebook-instagram. Acesso em: 7 jun. 2023.

HUGHES, Donna. The Internet and sex industries: Partners in global sexual exploitation. **IEEE Technology and Society Magazine**, Rhode Island, n. 19, p. 35-42, 01 Feb. 2000. Disponível em: https://www.researchgate.net/publication/3226679_The_Internet_and_sex_industries_Partners_in_global_sexual_exploitation. Acesso em: 6 ago. 2023.

HYUN, Jeonghee ; CHOI, Hanyong ; KIM, Jaesaeng. Deriving improvement plans through metaverse technology and implications. **International Journal of Intelligent Systems and Applications in Engineering**, [*S. l.*], n. 10, p. 197, 15 Oct. 2022. Disponível em: https://ijisae.org/index.php/IJISAE/article/view/2257. Acesso em: 6 ago. 2023.

IBM. **TCP/IP protocols**. New York: IBM, 2023a. Disponível em: https://www.ibm.com/docs/en/aix/7.2?topic=protocol-tcpip-protocols. Acesso em: 31 ago. 2023.

IBM. **What is a digital twin?** New York: IBM, 2023b. Disponível em: https://www.ibm.com/topics/what-is-a-digital-twin. Acesso em: 6 ago. 2023.

JOHNSON, Chris W. Anti-social networking: crowdsourcing and the cyber defence of national critical infrastructures. **Ergonomics**, London, n. 57, p. 419-433, 05 July 2013. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/00140139.2013.812749. Acesso em: 7 jun. 2023.

LEINER, Barry *et al.* A Brief History of the Internet. **ACM SIGCOMM Computer Communication Review**, Ithaca, v. 39, 23 Jan. 1999. Disponível em: https://arxiv.org/abs/cs/9901011. Acesso em: 6 ago. 2023.

MARCONI, Marina D. A.; LAKATOS, Eva M. **Fundamentos de Metodologia Científica**. 7. ed. São paulo: Atlas, 2010. 317 p.

MARLER, Timothy *et al.* **The Metaverse and homeland security**: opportunities and risks of persistent virtual environments. Santa Monica: RAND Corporation, 2023. Disponível em: https://www.rand.org/pubs/perspectives/PEA2217-2.html. Acesso em: 31 ago. 2023.

META. **AR/VR**: novas dimensões de conexão. [Miami]: Meta, 2023. Disponível em: https://www.facebook.com/business/news/insights/future-ar-vr. Acesso em: 10 mar. 2023.

META. **Introducing Meta**: a Social Technology Company. [Miami]: Meta, 2021. Disponível em: https://about.fb.com/news/2021/10/facebook-company-is-now-meta/. Acesso em: 7 jun. 2023.

METZ, Daniel; GURĂU, Maria-Mihaela. Emerging and disruptive technologies: the metaverse, implications on global security. **Land Forces Academy Review**, Sibiu, v. 27, p. 411-422, 2022. Disponível em: https://sciendo.com/pdf/10.2478/raft-2022-0050. Acesso em: 30 mar. 2023.

NAIR, Vivek; GARRIDO, Gonzalo M.; SONG, Dawn X. Exploring the unprecedented privacy risks of the metaverse. **ArXiv**, Ithaca, 26 July 2022. Disponível em: https://arxiv.org/abs/2207.13176. Acesso em: 7 jun. 2023.

NATIONAL SCIENCE FOUNDATION. **A Brief History of NSF and the Internet**. Alexandria, VA: NSF, 2003. Disponível em: https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050. Acesso em: 6 ago. 2023.

NATIONAL SCIENCE FOUNDATION. **The Day the World Changed**. Alexandria, VA: NSF, 2008. Disponível em:

https://www.nsf.gov/news/news_summ.jsp?cntn_id=111824. Acesso em: 6 ago. 2023.

NON-FUNGIBLE Tokens (NFTs) explained. **AWS**, 2023. Disponível em: https://aws.amazon.com/pt/blockchain/nfts-explained/. Acesso em: 30 mar. 2023.

OECD. **Digital Transformation in the Age of COVID-19**: building resilience and bridging divides. Paris: OECD, 2020. Disponível em: https://www.oecd.org/digital/digital-economy-outlook-covid.pdf. Acesso em: 30 ago. 2023.

ORACLE. **What is IoT**? Austin: Oracle, 2021. Disponível em: https://www.oracle.com/br/internet-of-things/what-is-iot/. Acesso em: 07 jun. 2023.

PAASONEN, Susanna. Online Pornography. *In*: WRIGHT, James D. (ed.). **International Encyclopedia of the Social & Behavioral Sciences.** 2. ed. Oxford: Elsevier, 2015. p. 217-222. Disponível em: https://www.researchgate.net/publication/304193827_Online_Pornography. Acesso em: 6 ago. 2023.

PAGLIUSI, Sérgio P. **Cibersegurança no metaverso e blockchain**. Rio de Janeiro: Clube Naval, 2023. 1 vídeo. (55 min.). Disponível em: https://www.youtube.com/watch?v=B8o3SzcrwO0. Acesso em: 7 jun. 2023.

PETROBRAS. **Petrobras avança no desenvolvimento do Campo de Búzios e assina contrato para construção da plataforma P-82**. [Rio de Janeiro]: Petrobras, 2022. Disponível em: https://petrobras.com.br/fatos-e-dados/petrobras-avanca-no-desenvolvimento-do-campo-de-buzios-e-assina-contrato-para-construcao-da-plataforma-p-82.htm. Acesso em: 6 ago. 2023.

REINO Unido decide banir TikTok de celulares de trabalho dos funcionários do governo. **Jornal Nacional**, 16 mar. 2023. 1 vídeo. (3 min.). Disponível em: https://globoplay.globo.com/v/11455734/. Acesso em: 26 ago. 2023.

ROSENBERG, Louis. The Metaverse and conversational AI as a threat vector for targeted influence. *In*: IEEE ANNUAL COMPUTING AND COMMUNICATION WORKSHOP AND CONFERENCE (CCWC), 13., 2023, Pismo Beach, CA. **Proceedings** […]. [California]: IEEE, 2023. Disponível em:

https://www.researchgate.net/publication/368492998_The_Metaverse_and_Conversational_AI_as_a_Threat_Vector_for_Targeted_Influence. Acesso em: 5 ago. 2023.

RUIZ, João Á. **Metodologia Científica**: guia para eficiência nos estudos. 6. ed. São Paulo: Atlas, 2006. 184 p.

SEOUL. Metropolitan Government. **Seoul to provide public services through its own metaverse platform**. Seoul: Metropolitan Government, 2021. Disponível em: https://english.seoul.go.kr/seoul-to-provide-public-services-through-its-own-metaverse-platform/. Acesso em: 31 ago. 2023.

STEPHENSON, Neal. **Snow crash**. 1. ed. São Paulo: Aleph, 2015. 390 p.

THOMPSON, Robin L. Radicalization and the Use of Social Media. **Journal of Strategic**, Rapid City, n. 4, p. 167-190, 10 Jan. 2012. Disponível em: http://scholarcommons.usf.edu/jss/vol4/iss4/9. Acesso em: 7 jun. 2023.

THORNBERRY, William M. **National Artificial Intelligence initiative act for fiscal year 2020**: Conference Report. Washington, DC: U.S. Government Publishing Office, 2020. Disponível em: https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1210. Acesso em: 31 ago. 2023.

UNITED STATES. White House. **National security strategy for a new century**. Washington, DC: White House, 1998. Disponível em: https://nssarchive.us/national-security-strategy-1998/. Acesso em: 6 ago. 2023.

VANORIO, Fabio. **Metaverse**: implications for security and intelligence. Rome: NATO Defense College Foundation, 2022. Disponível em: https://www.natofoundation.org/wp-content/uploads/2022/02/NDCF-Paper-Vanorio-110222.pdf. Acesso em: 6 ago. 2023.

VERGARA, Sylvia C. **Projetos e relatórios de pesquisa em administração**. 16. ed. São Paulo: Atlas, 2016.

VRIES, Katja de. Avatars out of Control. Gazira Babeli, pose balls and ‘rape’ in second life. *In*: GUTWHIRT, Serge *et al*. (ed.). **Computers, privacy and data protection**: an element of choice. Dordrecht: Springler, 2011. p. 233 - 250.

Disponível em: https://www.researchgate.net/publication/226652790_Avatars_Out_of_Control_Gazira_Babeli_Pose_Balls_and_Rape_in_Second_Life. Acesso em: 6 ago. 2023.

WEI, He. Future of internet virtually in sight. **China Daily**, 2 Nov. 2022. Disponível em: https://global.chinadaily.com.cn/a/202202/11/WS6205c99fa310cdd39bc860e0.html. Acesso em: 6 ago. 2023.

WHAT is blockchain? **Euromoney Learning**, London, 2023. Disponível em: https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain. Acesso em: 30 mar. 2023.

GLOSSÁRIO

5G - *Fifth Generation* = É a quinta geração de redes de dados para celulares. Até 100 vezes mais rápida que o atual 4G (ERICSSON, 2023a).

6G - *Sixth Generation* = É a sexta geração de redes de dados para celulares. Estima-se que será até 100 vezes mais rápida que o 5G. A previsão de implementação da tecnologia é para 2030 (ERICSSON, 2023b).

AI - *Artificial Intelligence* = Inteligência Artificial (IA). Sistema baseado em máquina que pode, para um determinado conjunto de objetivos definidos pelo homem, fazer previsões, recomendações ou decisões que influenciam ambientes reais ou virtuais. Os sistemas de inteligência artificial utilizam informações baseadas em máquinas e humanos para: perceber ambientes reais e virtuais; abstrair tais percepções em modelos por meio de análise de forma automatizada; e usar inferência de modelo para formular opções de informação ou ação (THORNBERRY, 2020).

AR - *Augmented Reality* = Realidade aumentada. Tecnologia em que informações digitais (objetos) são sobrepostas ao mundo físico, geralmente por meio de um dispositivo como uma câmera, TV ou um *smartphone* (META, 2023).

AVATAR - Imagem eletrônica que representa e pode ser manipulada por um usuário de computador. O termo avatar deriva de uma palavra em sânscrito que significa "descida" e quando apareceu pela primeira vez em na língua inglesa, no final do século XVIII, referia-se à descida de uma divindade à terra - normalmente, a encarnação na forma terrena de Vishnu ou outra divindade hindu. Mais tarde, passou a se referir a qualquer encarnação na forma humana e, em seguida, a qualquer encarnação (como a de um conceito ou filosofia), seja ou não na forma de uma pessoa. Na era da tecnologia, avatar desenvolveu um outro sentido – agora o termo pode ser usado para a imagem que uma pessoa escolhe como sua “corporificação” em um meio eletrônico (AVATAR, 2023).

B5G - *Beyond* 5G = rede de dados para celulares até cinco vezes mais rápida que o 5G (ERICSSON, 2023a).

BLOCKCHAIN - é um protocolo de registro de informações, de uma forma que torna difícil ou impossível alterar, hackear ou enganar o sistema. Tem sido essencialmente empregado como um livro digital de transações, que é duplicado e distribuído por toda a rede de sistemas de computador no *blockchain*. Cada bloco na cadeia contém uma série de transações, e toda vez que uma nova transação ocorre na *blockchain*, um registro dessa transação é adicionado ao registro de cada participante. Atualmente é muito empregado no mercado de criptomoedas (WHAT is..., 2023).

IoT - *Internet of Things* = Internet das coisas. Rede de objetos físicos incorporados a sensores, software e outras tecnologias com o objetivo de conectar e trocar dados com outros dispositivos e sistemas pela internet. Esses dispositivos variam de objetos domésticos comuns a ferramentas industriais altamente sofisticadas (ORACLE, 2021).

NON-FUNGIBLE TOKENS - *Tokens* não fungíveis, geralmente chamados de NFTs, são *tokens* baseados em *blockchain*, cada um representando um ativo exclusivo, como uma obra de arte, conteúdo digital ou mídia. Um NFT pode ser pensado como um certificado digital irrevogável de propriedade e autenticidade de um determinado ativo, seja ele digital ou físico. NFTs são projetados para serem criptograficamente verificáveis, únicos ou escassos e facilmente transferíveis. Aproveitando as assinaturas criptográficas nativas do *blockchain* no qual um NFT é emitido, pode-se determinar facilmente a origem e o atual proprietário do ativo em questão em segundos (NON-FUNGIBLE…, 2023).

TCP/IP - *Transmission Control Protocol/Internet Protocol* – conjunto de protocolos, concebido em termos de camadas, os quais definem os conjuntos de regras para formatos de mensagens e procedimentos que permitem que máquinas e programas aplicativos troquem informações. Essas regras devem ser

seguidas por cada máquina envolvida na comunicação para que o computador receptor possa compreender a mensagem (IBM, 2023a).

VR - *Virtual Reality* = Realidade virtual. Tecnologia que permite uma experiência totalmente imersiva, por meio de dispositivos como um *headset*, que imerge os sentidos do usuário em um universo virtual (META, 2023).