Prática de Exercícios Cibernéticos Simulados para Seleção e Preparo: Estudo de Caso - *MANDABYTE* e SIMOC

Luiz Henrique Filadelfo Cardoso[1] e Tiago Josué Diedrich[2]
[1]Gabinete do Comandante da Aeronáutica (GABAER), Brasília/DF - Brasil
[2]Núcleo do Centro de Defesa Cibernética da Aeronáutica (NuCDCAER), Brasília/DF - Brasil

***Resumo*— Este estudo tem como objetivo analisar duas alternativas para a seleção de novos talentos na área de Defesa Cibernética (DefCiber) e, ao mesmo tempo, sugere formas de treinamento contínuo a militares especializados no domínio em comento, por meio de simulações virtuais, quais sejam: Competição Cibernética das Forças Armadas (FA), conhecida como *Mandabyte*; e o Simulador de Operações Cibernéticas (SIMOC). Em relação à primeira, verificou-se a necessidade de aperfeiçoamentos na organização para se expandir o alcance da referida competição, não só ao âmbito das FA, mas a todo setor público e privado brasileiro responsável pela segurança de ativos cibernéticos críticos. Já ao que se refere à segunda alternativa, identificaram-se oportunidades para disponibilização de acesso regular a um universo maior de combatentes cibernéticos já formados e atuantes na área de DefCiber, sobretudo egressos dos Cursos de Guerra Cibernética, já ministrados pelo Exército Brasileiro (EB).**

***Palavras-Chave*— Defesa Cibernética, Exercícios Virtuais, Capacitação Militar**

I. Introdução

O ano de 2023 apresenta um cenário dominado por ameaças cibernéticas avançadas capazes de sequestrar, exfiltrar e corromper grandes quantidades de dados pessoais e governamentais [1]. Isso sugere uma urgente preocupação para a nação brasileira, a qual deve possuir profissionais altamente qualificados, que possam atuar de maneira oportuna e efetiva quando concitados a agir no domínio cibernético.

No entanto, como selecionar e preparar os combatentes responsáveis por prover a DefCiber no Brasil? Quais são os critérios utilizados para preparar os profissionais encarregados da Defesa Cibernética no país? Quais são as estratégias empregadas para simular as complexidades e particularidades do ciberespaço de forma mais realista? Existem parcerias ou colaborações com instituições especializadas no setor privado ou acadêmico para permitir a capacitação dos profissionais de DefCiber?

Frente a esses questionamentos, surgem como oportunas as soluções suportadas por simulação, principalmente por serem capazes de proverem cenários controlados, customizáveis, com qualidade e a um menor custo para o preparo contínuo de combatentes atuantes no ciberespaço.

Nesse ponto, devido à necessidade de melhor entendimento da estrutura administrativa e operacional do setor cibernético brasileiro, tal qual apontado em [2] e [3], além do suporte argumentativo no decorrer deste estudo, cabe apresentar a correlação subordinativa entre as Organizações Militares (OM) do EB responsáveis pela Defesa Cibernética nacional, quais sejam: Comando de Defesa Cibernética (ComDCiber), Centro de Defesa Cibernética (CDCiber) e a Escola de Defesa Cibernética (ENaDCiber), como apresentado na Fig. 1.

Luiz Henrique Filadelfo Cardoso, luizhenriquelhfc1@fab.mil.br; Tiago Josué Diedrich, diedrichtjd@fab.mil.br.

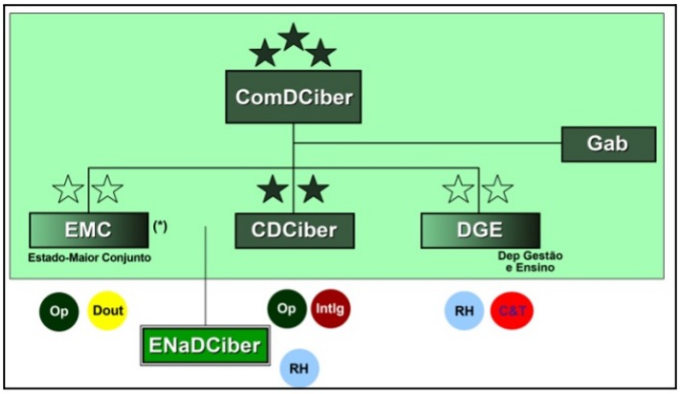

Fig. 1: Organizações do EB responsáveis pelo Programa Estratégico de Defesa Cibernética [4]

Para tanto, este artigo foi organizado da seguinte forma: na Seção II, definem-se simulação e exercícios simulados virtuais, assim como são apresentados, conceitualmente, exercício de dupla ação e exercício tipo Captura de Bandeira (do inglês, *Capture The Flag – CTF*); na Seção III, são analisadas as duas principais alternativas hoje existentes para a seleção e treinamento de combatentes cibernéticos brasileiros: *Mandabyte* e SIMOC; já, na Seção IV, são analisados e apresentados os principais aspectos e procedimentos que podem ser adaptados e (ou) aperfeiçoados para se obterem maior efetividade, eficiência de meios e alcance em tais soluções; e, por fim, na Seção V, são tecidas considerações finais após o estudo realizado.

II. Simulação e Exercícios Simulados Virtuais

[5] entende que a simulação é "*a imitação de uma operação ou processo existente no mundo real*", e, por conseguinte, simulacros são "*cópias que representam elementos que nunca existiram ou que não possuem mais o seu equivalente na realidade*".

Já para [6], simulação pode ser entendida como o processo capaz de "*modelar sistemas reais e conduzir experimentos com o propósito de entender o comportamento dos sistemas e avaliar várias estratégias para as suas operações*"; e simulador como sendo "*um aparelho e (ou) programa de computador capaz de reproduzir o comportamento de um determinado sistema*" existente no mundo real.

Ainda em [6], entende-se que a simulação pode ser utilizada como relevante meio de treinamento, e, dessa forma, pode ser classificada nas seguintes categorias:

- Simulações reais ou ao vivo: são aquelas executadas com sistemas reais e operadores reais, com o objetivo de treinar situações hipotéticas. São exemplos dessa classificação qualquer Exercício Operacional (ExOp) ou Manobra militar.
- Simulações virtuais: são aquelas onde o operador real utiliza um sistema modelado em ambiente virtual, emulando o comportamento dos sistemas de interesse. Simulador de voo para treinamento de pilotos de aeronaves é um exemplo dessa categoria.
- Simulações construtivas: são aquelas onde tanto os operadores quanto os sistemas são virtuais, concebidos mediante modelos matemáticos que buscam representar como os sistemas reais vão se comportar. Usualmente não se emprega hardware real, mas pode-se utilizar parte do software real dos sistemas de interesse, tornando ainda mais fidedignas as simulações realizadas. São exemplos, os simuladores MARTE, da Força Aérea Brasileira (FAB) e COMBATER, do EB.

Dessa forma, entende-se que, no meio militar, por possuir características, necessidades e objetivos particulares, a opção por simulações virtuais (computacionais) revestem-se de benefícios por prover economia de recursos, possibilidade de repetição (e customização) de cenários para aprendizado e menor risco do que a execução de um treinamento de combate que utilizaria equipamentos, pessoas e recursos reais [6].

Logo, a conformação de exercícios simulados computacionais customizados e criados especificamente para preparo dos militares responsáveis pela DefCiber brasileira reside como meio ideal para manter a perícia técnica e a capacidade de pronto-emprego em nível adequado para responder às demandas emergentes, dinâmicas e complexas de tal tarefa. No âmbito da FAB, tal reflexão foi inicialmente abordada em [7] e [8], ocasião em que os autores não só traçam um panorama da capacitação em Defesa Cibernética no Brasil, mas também listam os benefícios inerentes da adoção de um Exercício Operacional Cibernético Simulado (ExOpCiberSIM) regular no âmbito da FAB, que pode ser aplicado no contexto da CRUZEX *Flight* ou CRUZEX Comando e Controle (C2).

Nessa direção, há de se pontuar que algumas das características necessárias para entender e atuar no ciberespaço, como a complexidade de redes e ativos, pensamento crítico e o raciocínio técnico-lógico, são passíveis de serem emulados (e aperfeiçoados) por meio da adoção de exercícios simulados virtuais específicos, sobretudo a partir dos formatos *Red Team and Blue Team (RTBT)* e CTF, como será visto a seguir.

A. Exercício de Dupla Ação: RTBT

Conforme exposto por [9], um exercício RTBT consiste, basicamente, em um grupo de profissionais de segurança da informação (*Red Team*) intentar atacar e explorar uma infraestrutura cibernética, e outro (*Blue Team*), em lado oposto, ser capaz de se contrapor e proteger a infraestrutura sob ataque. Entende-se, assim, que dois objetivos principais devem ser atendidos durante tal exercício: (1) identificar vulnerabilidades na infraestrutura cibernética (emulada ou real) sob teste e (2) refinar as habilidades dos profissionais alocados em ambos os lados em combate simulado. Ao final do treinamento, deve-se realizar uma reunião no formato de *debriefing*, para que ambos os times apresentem suas considerações, pontos fortes e fracos identificados, assim como as estratégias e as táticas utilizadas durante o exercício, de forma a aperfeiçoar as competências técnicas – Técnicas, Táticas e Procedimentos (TTPs) – de todos os envolvidos.

Alguns elementos-chave para o sucesso do exercício consistem em: um *Red Team* hábil, que possua um extenso repertório de conhecimento e experiência, TTPs avançadas, uma mentalidade ofensiva e "fora da caixa" para resolver problemas, similar à postura de um oponente do mundo real (criminoso cibernético); uma equipe *Blue Team* atualizada e que possua conhecimento avançado não só em relação aos serviços, redes e sistemas a serem protegidos durante o exercício, mas também sobre o comportamento das ameaças cibernéticas mais atuais [9].

Importante destacar que um treinamento RTBT pode ser realizado nas modalidades de simulação real ou virtual. Esta última é a mais adequada quando se busca manter a integridade, a disponibilidade e a segurança dos ativos durante o exercício, bem como maior variedade de cenários a serem testados e explorados. [8].

B. Capture The Flag

O termo CTF designa um espectro de competições que exigem diversas habilidades dos competidores para a resolução de desafios "*challs*" (do inglês, *challenge*) relacionados à segurança da informação, com o objetivo de "capturar uma bandeira" - informação ou dica para pontuar e seguir no jogo. Tais desafios são divididos em categorias como: criptografia, esteganografia, análise de binários, engenharia reversa, programação, segurança de dispositivos móveis, análise de tráfego de redes, vulnerabilidades em aplicações web, análise forense, protocolo de redes Wi-Fi etc [10].

De acordo com [11], existem três tipos básicos de CTFs:

a) Jeopardy-Style: neste são apresentadas questões (*quizzes*) de diversas categorias, níveis de dificuldade e pontuações. A pessoa ou equipe (geralmente multidisciplinar, de três a cinco integrantes) que sairá campeã do CTF é a que resolver a maioria das questões (sobretudo aquelas de maior complexidade) e em menor tempo que os adversários. Em alguns CTF's, o acesso a outros *challs* é condicionado à resolução de anteriores, de menor complexidade, dentro da mesma categoria.

b) Ataque-defesa (*attack-defense*): de forma genérica, as equipes recebem uma rede própria ou apenas um host (máquina virtual) com diversos serviços (alguns com vulnerabilidades conhecidas) e ficam encarregadas de corrigir as vulnerabilidades em seus serviços e (ou) de desenvolver ferramentas (*exploits* e *payloads*) para atacarem a rede ou sistemas oponentes. O objetivo é atacar os pontos fracos da equipe rival (capturar as bandeiras alheias) e proteger-se contra ataques da outra equipe (defender suas bandeiras).

c) Formato misto: CTFs mistos podem variar de formato, mas geralmente consistem em uma configuração de jogo baseado em ataque-defesa, na qual as flags são questões típicas do estilo Jeopardy. Ou seja, a progressão nesse tipo de CTF não reside apenas em se explorar os serviços da equipe rival, mas também na habilidade de resolver as questões presentes nas flags capturadas.

III. Estudo de Caso: *Mandabyte* e SIMOC

Atento às características e particularidades presentes nesses formatos de competições e exercícios cibernéticos descritos na seção anterior, e como eles podem contribuir para a seleção, preparo e melhor diálogo com o combatente do século XXI, o EB adotou como principais soluções para atender tais demandas a Competição de *Mandabyte* e o SIMOC.

A. *Mandabyte*

A partir da ideia inicial e coordenação voluntária de alguns militares do EB com experiência em competições cibernéticas nacionais e internacionais, sobretudo na modalidade CTF, e da percepção quanto à necessidade em se desenvolver uma competição similar voltada a identificar recursos humanos das FA brasileiras para atuar na DefCiber, o CDCiber sugere no ano de 2016 a Competição de Cibernética das Forças Armadas, o que hoje conhecemos como *Mandabyte* [12].

A respeito do *Mandabyte*, o Tenente-Coronel Righi, à época integrante do ComDCiber, destacou que a competição oferece uma oportunidade valiosa para que os competidores apliquem seu conhecimento adquirido na área de cibernética, além de proporcionar uma chance de praticar o que foi aprendido, o que é frequentemente uma dificuldade nesse campo de atuação [13].

Desde sua criação, ocorreram nove competições do *Mandabyte*: duas em 2016 (1.0 e 2.0), duas em 2017 (3.0 e 4.0), uma em 2018 (V), uma em 2019 (6ª edição), uma no ano de 2020 (7ª edição), uma em 2021 (8ª edição, primeira edição como fase preparatória para o Exercício Guardião Cibernético - EGC) e uma edição no ano de 2022 (9ª edição). A edição mais recente contou com a participação de 133 equipes, totalizando 300 competidores militares e civis responsáveis pela segurança cibernética de infraestruturas críticas, em âmbito privado e governamental [12], [14], [15].

Destarte, observa-se que os desafios do *Mandabyte* devem ser resolvidos dentro de seis horas ininterruptas de competição e são relacionados, basicamente, aos temas de Criptografia, Forense Computacional, Pentest em Aplicações Web, e Engenharia Reversa e Miscelânea. Na Fig. 2, é possível observar a reprodução de tela contendo a quantidade de participantes e outras informações de interesse sobre a 9ª edição *Mandabyte* realizada no dia 17 de julho de 2022.

Fig. 2: Informações sobre a 9ª Edição *Mandabyte* [15]

Quanto aos aspectos organizacionais, cabe expor que até o ano de 2019 o cadastramento das equipes e a montagem dos desafios eram desenvolvidos entre militares voluntários do EB, assim como, a infraestrutura física e lógica eram hospedadas no 11º Centro de Telemática na cidade de Curitiba-PR, cabendo ao ComDCiber o fomento e a divulgação do referido evento aos integrantes da Marinha do Brasil (MB), EB e FAB. A partir da 7ª edição, toda a responsabilidade (administrativa e operacional) pela organização do *Mandabyte* passou a ser do ComDCiber e seus órgãos subordinados [12].

Hoje, em específico, a infraestrutura lógica e física para a realização do *Mandabyte* e a disponibilização de seus "challs" resumem-se, sinteticamente, em um servidor/Datacenter com software de virtualização instalado, no qual também está alocado um firewall que cuida da segurança e da criação e gestão das chaves assimétricas, que permitem estabelecer conexão (*Virtual Private Network* – VPN) entre as equipes competidoras e o ambiente de competição. Por meio de *hosts* virtualizados, alocados em redes segregadas, disponibilizam-se o ambiente de interação da competição e inserção das flags, assim como com máquinas virtuais vulneráveis destinadas a servirem de base para os desafios disponibilizados. Ao passar das edições, também se observa a contínua necessidade de expansão da capacidade de processamento, memória útil e link internet para o CTF devido ao acentuado aumento do número de participantes inscritos a cada nova competição [12], [14].

B. *SIMOC*

Considerando a premissa de que o espaço cibernético possui características que o distingue de outros domínios e, por esse motivo as ferramentas, técnicas e procedimentos utilizados em outros domínios podem não surtir efeito adequado por ser um ambiente eminentemente virtual (ainda que seus efeitos possam ser sentidos no real), o EB identificou a necessidade de possuir uma ferramenta customizada e baseada em simulação, que pudesse atuar de forma segura, controlada e em auxílio ao processo de formação dos profissionais responsáveis pela DefCiber nacional [16].

Fruto dessa necessidade, após avaliação criteriosa de diversas outras soluções de mercado, optou-se pelo SIMOC, desenvolvido de maneira colaborativa entre a indústria nacional e instrutores do Centro de Instrução de Guerra Eletrônica (CIGE), tal qual citado por [16]. Na Fig. 3 é possível perceber representação de tela do SIMOC.

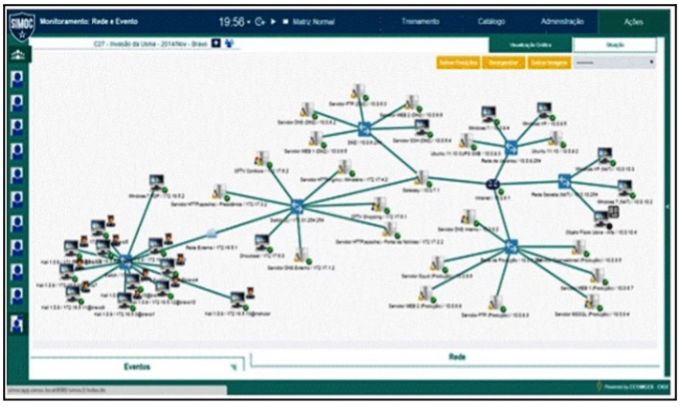

Fig. 3: Tela SIMOC [16]

Importa mencionar que o SIMOC surgiu com o objetivo de ser uma ferramenta baseada em simulação virtual, estocástica e dinâmica, capaz de fornecer treinamentos em configuração e administração de redes; operações cibernéticas de ataque e

defesa a redes TCP/IP, sistemas operacionais e (ou) aplicações instaladas nas máquinas e demais dispositivos existentes e possíveis de serem emulados do mundo real [17]. Para isso, conforme apontado em [16], o SIMOC faz uso de máquinas virtuais (computadores e dispositivos de rede) em auxílio ao processo de treinamento, cujas máquinas desejadas para configurar uma rede são selecionadas e relacionadas entre si. Para a criação da rede pode-se especificar as configurações na forma de *scripts* que serão assim executados nas máquinas virtuais. Todos os elementos usados na criação da rede são modulares, permitindo a reutilização e facilitando a expansão do conteúdo disponível, inclusive para utilização de outros alunos e em outros cenários de treinamento. O principal objetivo é fornecer uma ferramenta para geração automática de redes virtualizadas com acesso a partir da interface web.

Outra característica relevante do SIMOC, que estimula e aperfeiçoa o aprendizado, é a sua capacidade de integrar objetos físicos do mundo real aos seus modelos e redes virtualizadas. Assim, a partir de ações e procedimentos cibernéticos realizados nos modelos virtuais do simulador também é possível emular efeitos cinéticos do mundo real [18]. Por exemplo, tal qual presente na Fig. 4, é possível perceber a representação em escala de uma usina termoelétrica utilizada em treinamento, na qual alunos puderam interagir e interferir em sua operação, bastando para isso acessar as redes e computadores (emulados em máquinas virtuais) específicos para seu funcionamento dentro de um cenário virtual disponibilizado pelo SIMOC.

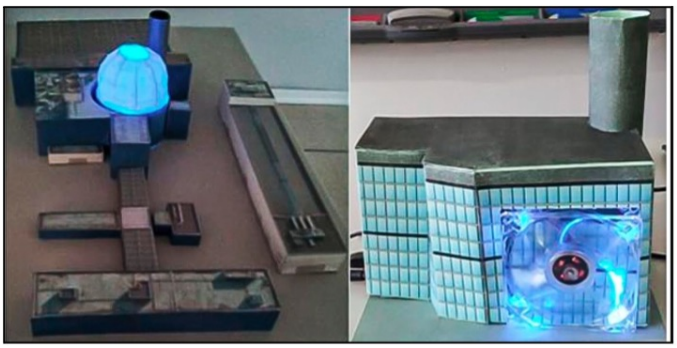

Fig. 4: Maquete de usina termoelétrica utilizada em treinamento SIMOC [16]

Importante acrescentar que, conforme detalhado por [18], a utilização do SIMOC tem se mostrado relevante no processo de ensino e aprendizagem do domínio cibernético, apresentando as seguintes vantagens:

a) Possibilidade de criar diversos tipos de simulações tais como: exercícios de dupla ação, criação de redes de computadores (a partir de uma situação-problema) e a gerência de uma rede de dados;
b) Reuso de elementos (objetos, eventos, métricas etc.) pré-registrados no catálogo do simulador, com o objetivo de adequar o cenário a uma situação-problema ou de criar uma nova;
c) Capacidade de se criar redes mistas, contendo segmentos virtuais e segmentos de rede e artefatos reais;
d) Variedade de funcionalidades que apoiam o instrutor durante as simulações, tais como: gerador de tráfego randômico, defesa automatizada, ataque automatizado, recurso de gravação, material de apoio e aplicação das diversas métricas existentes;
e) Monitoramento em tempo real com a possibilidade de interferência do instrutor durante a execução dos exercícios. Como exemplo, o instrutor pode: pausar a simulação; adiantar, repetir uma situação; mudar parte do cenário; e modificar o nível de dificuldade do exercício;
f) A implementação do simulador conta com uma relativa segurança na sua infraestrutura, seja para o acesso interno (administrador, instrutor, alunos) ou para acessos externos ou remoto;
g) A utilização de maquetes, conectadas ao simulador, propicia ao instruendo a possibilidade de emular a consequência "real" de um ataque cibernético, realizado pelo aluno, sobre a infraestrutura de uma localidade (fábrica, cidade etc.); e
h) O simulador pode ser acessado, remotamente, permitindo a realização de treinamento de militares em diferentes localidades.

No entanto, conforme também destacado em [18] e [9], o SIMOC encontra algumas limitações, tais como:

a) Inviabilidade de simular ligações de fibra ótica. No entanto, essa limitação pode ser parcialmente contornada com a integração de redes de fibra óticas reais ao SIMOC;
b) As principais empresas fornecedoras de soluções de TI não disponibilizam as versões virtualizadas de seus produtos. Uma possibilidade para contornar esse problema seria fazer parcerias com as empresas para obter os produtos de interesse no formato virtual. Por exemplo, atualmente, existe a possibilidade de virtualizar roteadores da empresa CISCO. Contudo, para realizar essa virtualização, depende-se de autorização prévia da empresa e (ou) obtenção de licenças;
c) O simulador não é um ambiente adequado para a análise de vírus de computador, uma vez que *malwares* avançados e *Advanced Persistent Threats* (APTs) são capazes de identificar a existência de máquinas virtuais, e nesse caso, sendo capazes de evadir e (ou) não executarem seus códigos e rotinas maliciosas; e
d) Atualmente, não é possível conectar o SIMOC às máquinas pessoais dos alunos para realizar os exercícios. Esse fato acaba se tornando um óbice, pois é comum que esses instruendos já possuam, em suas máquinas, suas ferramentas instaladas e customizadas para as atividades no ciberespaço.

IV. Análise

Dado todo o contexto, ainda que o *Mandabyte* e o SIMOC representem importantes avanços e casos de sucesso para a seleção e preparo de novos combatentes cibernéticos, há de se ter um olhar crítico para reconhecer oportunidades quanto aos aspectos que possam vir a torná-los mais acessíveis a um universo maior de profissionais (não só aqueles em formação ou integrantes de operações militares pontuais), e, com isso, proporcionar uma contínua capacitação a partir da simulação e de desafios cibernéticos customizáveis.

No tocante ao *Mandabyte*, ainda que o esforço colaborativo inicial aliado à contribuição institucional do ComDCiber tenha trazido a competição até aqui com qualidade, economia de meios e formato atrativo, é necessário refletir sobre sua evolução e formato de apoio caso o objetivo seja aperfeiçoar e

expandir o referido CTF para um espectro maior de equipes, bem como prover maior regularidade e complexidade aos desafios a serem disponibilizados.

A existência de equipe permanente e dedicada para gerir especificamente o *Mandabyte* (infraestrutura, mapeamento e gestão de talentos identificados; divulgação, confecção e catalogação de desafios etc.), formado por integrantes das três Forças Singulares, não só traria benefícios implícitos advindos da gerência institucional, mas também seria capaz de gerar continuidade e eficácia na gestão e repasse de conhecimento para outros profissionais em relação à experiência adquirida a partir do processo de organização e realização do referido CTF militar.

Assim, sugere-se a possibilidade da ENaDCiber assumir a formação, o apoio e a manutenção de uma equipe dedicada à gestão do *Mandabyte* e outras competições cibernéticas em múltiplos formatos, com base em simulação, e sob a supervisão do ComDCiber. A conclusão é baseada na compatibilidade dos objetivos do *Mandabyte* com a missão da ENaDCiber, que é capacitar recursos humanos para atuar no setor cibernético em defesa do país e se tornar um centro de excelência em ensino e pesquisa de Defesa Cibernética em nível nacional [3].

Já no que concerne ao SIMOC, cabe refletir que, mesmo que tenha sido desenvolvido inicialmente para atender às demandas do CIGE, com seu emprego focado para o Curso de Guerra Cibernética (para graduados e para oficiais), sua utilização deve ser incentivada e expandida para além dos alunos em formação, sobretudo para os profissionais de DefCiber já em atuação no âmbito das outras FA e setores de interesse.

Esse argumento ganha força devido à falta de oportunidades para exercícios regulares ou treinamento prático constante em ambientes simulados virtuais para a maioria dos militares especializados em Defesa Cibernética. No entanto, é essencial manter a constante preparação dessas equipes para que estejam prontas para agir quando necessário.

Uma alternativa ao cenário exposto anteriormente seria o estabelecimento de acordos entre as OM que possuem militares especializados (e a DefCiber como missão) com o CIGE, sob coordenação da ENaDCiber, para estabelecer um calendário regular e customizado para treinamento no SIMOC e (ou) outra solução adotada para exercícios simulados. De maneira similar ao que ocorre com militares em outras atividades específicas (tais como piloto de aeronaves, controlador de tráfego aéreo etc.), propõe-se a definição de um número específico de horas a serem cumpridas em simulador. De acordo com a natureza da missão de certas OM (ataque, exploração ou proteção cibernética) sugerem-se a definição de cenários, a melhor forma de acesso ao simulador (remoto ou local), carga de treinamento e metas a serem atingidas durante os treinamentos para a elevação operacional dos combatentes cibernéticos em aperfeiçoamento.

Desse modo, com a adoção de um calendário de treinamento customizado e em simulador específico para combatentes cibernéticos em atividade, não só seria possível aumentar a eficiência e a taxa de retorno de investimento em pessoal e na manutenção do simulador, mas também proporcionar o preparo contínuo e de qualidade daqueles que tem o dever de estarem preparados para serem empregados na defesa das redes, sistemas e plataformas militares acessíveis pelo domínio cibernético, 24 horas por dia, 7 dias por semana, em qualquer lugar e em quaisquer condições.

V. Conclusões

Ao se inspirar na essência da expressão: "*Você luta como treinou*", este artigo revisou analiticamente duas soluções, *Mandabyte* e SIMOC, a fim de identificar possíveis aspectos que possam ser aperfeiçoados para prover maior alcance e eficiência de meios, sobretudo para a seleção de novos combatentes e preparo contínuo de militares a serem empregados no âmbito cibernético.

Para alcançar esse objetivo, além de abordar a importância de ter combatentes capacitados no campo cibernético, também foram discutidos conceitos relacionados à simulação, exercícios simulados, CTF e RTBT. Esses conceitos serviram de base para a análise posterior das soluções abordadas neste artigo.

Em relação ao *Mandabyte*, identificou-se a necessidade de criar uma equipe ou seção dedicada diretamente ao ENaDCiber, responsável por organizar e gerenciar essa competição tanto em termos tecnológicos quanto administrativos. Essa configuração é considerada recomendável para que, com base nos conhecimentos adquiridos e nas lições aprendidas com esse pioneiro CTF militar, seja possível documentar desafios e processos (gestão do conhecimento), realizar edições de forma mais regular, gerenciar infraestrutura e expandir o formato atual, visando ampliar o alcance, a complexidade e a diversidade dos desafios.

Além disso, essa equipe poderia explorar a possibilidade de viabilizar outras opções também baseadas em jogos cibernéticos simulados, como exercícios de dupla reação, que possam oferecer incentivos para hackers éticos. Essas atividades não se restringiriam apenas ao público militar do EB, mas também seriam úteis para apoiar outras FA e profissionais civis especializados em setores de interesse, como bancos, segurança pública, energia, setor nuclear, entre outros.

No que diz respeito ao SIMOC, observou-se a falta de acesso a um maior número de profissionais cibernéticos que já concluíram sua formação e estão empregados na área de DefCiber. Identificou-se, assim, uma oportunidade de criar um calendário anual coordenado entre o CIGE e a OM interessada das três FA para obter suporte de treinamento do SIMOC ou outra solução ou sistema baseado em simulação, preenchendo o intervalo entre os cursos de formação em guerra cibernética para oficiais e graduados. Isso permitiria utilizar plenamente a plataforma para realizar exercícios cibernéticos personalizados e aprimorar as habilidades do pessoal. Nesse sentido, a atuação administrativa e coordenativa da ENaDCiber também se mostra essencial.

Por fim, como perspectiva para pesquisas futuras, considera-se a necessidade de aprofundar os estudos para encontrar a melhor abordagem de treinamento contínuo de combatentes cibernéticos em simuladores, adaptados a cada força armada e suas necessidades específicas. Na FAB, após a criação do Centro de Defesa Cibernética da Aeronáutica (CDCAER), surgem questões importantes a serem respondidas: qual seria a quantidade ideal de horas em simulador para preparar adequadamente os operadores cibernéticos para suas missões reais? Quais cenários e sistemas devem ser simulados (como sistemas de radar, sistemas embarcados em plataformas aéreas, protocolos de comunicações, satélites de comunicações militares e estações de solo, sistemas de controle de tráfego aéreo etc.)? Esses cenários seriam padronizados ou personalizados com base na natureza da missão (ataque, exploração ou proteção)?

Seria possível medir a eficiência do combatente cibernético com base no tempo de treinamento em simulador, assim como ocorre com pilotos militares e controladores de tráfego aéreo?

Em suma, a resiliência cibernética conquistada por meio da devida resposta e da implementação dessas questões tem o potencial de elevar o preparo e a eficácia do combatente cibernético brasileiro a um nível inédito, capacitando-o com as competências necessárias para enfrentar os desafios, tecnologias e complexidades intrínsecas às ameaças cibernéticas da atualidade.

REFERÊNCIAS

[1] L. Cardoso, "Anatomia de um ataque cibernético: conhecer e entender para melhor defender os ativos e meios de interesse da força aérea brasilieira," *SPECTRUM: Revista do Comando de Preparo*, no. 20, pp. 51–57, 2017.

[2] Brasil. Ministério da Defesa, "Estratégia nacional de defesa (end)," DECRETO Nº 6.703, de 18 de DEZ 2008, 2008, brasília. [Online]. Available: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm

[3] Brasil. Comando da Aeronáutica. DCA 11-130, "Diretriz de implantação do núcleo do centro de defesa cibernética da aeronáutica," Comando da Aeronáutica, Brasília, DF, Tech. Rep., out 2020.

[4] M. F. C. Marra, "Programa de defesa cibernética na defesa nacional," in *XV Congresso Acadêmico sobre Defesa Nacional*, 2018, acesso em 11 jun. 2023. [Online]. Available: https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/palestra_cadn_xi/xv_cadn/programaa_daa_defesaa_ciberneticaa_naa_defesaa_nacional.pdf

[5] J. Baudrillard, *Simulacros e Simulação*. Lisboa: Antropos, 1991.

[6] R. N. L. Nogueira, G. M. L. Filho, and A. G. R. Werneck, "Simulação para o preparo da força aérea," *PREPARO: Revista do Comando de Preparo*, no. 1, pp. 4–10, 2018.

[7] T. J. Diedrich, A. F. A. Machado, and P. R. M. Oliveira, "Capacitação de pessoal na área de defesa cibernética no âmbito do comando-geral de operações aéreas," *SPECTRUM: Revista do Comando-Geral de Operações Aéreas*, no. 18, pp. 11–16, set. 2015.

[8] T. J. Diedrich, A. C. Gonçalves, and R. C. B. da Silva, "Simulação cibernética e a capacitação de pessoal para operações militares no ciberespaço," *SPECTRUM: Revista do Comando-Geral de Operações Aéreas*, vol. 19, pp. 53–58, setembro 2016.

[9] R. Mejia, "Red team, blue team: How to run an effective simulation," https://www.networkworld.com/article/2278686/lan-wan/red-team--blue-team--how-to-run-an-effective-simulation.html?page=1, 2008, acesso em 18 jun 2023.

[10] CTF-TIME, "What is capture the flag," https://ctftime.org/ctf-wtf/, 2015, acesso em 10 jun 2023.

[11] CTF-BR, "CTFS," https://ctf-br.org/sobre/, acesso em 11 jul. 2023.

[12] E. L. O. Gonçalves, "Aspectos envolvidos na criação e desenvolvimento da competição de cibernética da forças armadas (mandabyte)," 2020, questionário de perguntas encaminhado via email. Colhido em 22/10/2020. Entrevistador: Luiz Henrique Filadelfo Cardoso.

[13] Exército Brasileiro, "Terceira competição de cibernética das forças armadas," https://www.eb.mil.br/exercito-brasileiro?p_p_id=101&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_101_struts_action=%2Fasset_publisher%2Fview_content&_101_assetEntryId=8194173&_101_type=content&_101_groupId=8032597&_101_urlTitle=terceira-competicao-de-cibernetica-das-forcas-armadas&inheritRedirect=true, 2017, acesso em 18 jul. 2023.

[14] E. BRASILEIRO. (2020) 7ª edição de competição cibernética entre integrantes das forças armadas busca novos talentos na área. [Online]. Available: https://www.eb.mil.br/exercito-brasileiro?p_p_id=101&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_101_struts_action=%2Fasset_publisher%2Fview_content&_101_assetEntryId=12363209&_101_type=content&_101_groupId=8032597&_101_urlTitle=7-edicao-de-competicao-cibernetica-entre-integrantes-das-forcas-armadas-busca-novos-talentos-na-area&inheritRedirect=true

[15] Dciber.org, "Instituto ctem+ realizou a competição ctf (capture the flag) mandabyte 2022," https://dciber.org/instituto-ctem-realizou-a-competicao-ctf-capture-the-flag-mandabyte-2022/, 2022, acesso em 18 jul. 2023.

[16] A. F. A. Machado, F. A. C. Regueira, and J. Rezende, "Use of simulation to achieve better results in cyber military training," in *MILCOM: Military Communications Conference*. IEEE Communications Society, 2015, pp. 1270–1275.

[17] R. Gomes, "Simulador de operações de guerra cibernética," Exposição Oral, 2013.

[18] A. F. Machado, "Utilização de simuladores para a formação de guerreiros cibernéticos," 2017. [Online]. Available: https://www.publicacoesacademicas.uniceub.br/gti/article/viewFile/4322/3635