Simulador de Ações Cibernéticas (SACi), o Cyber Range do Exército Brasileiro: preparando as Forças Armadas para os desafios cibernéticos do século XXI.

Major Rodrigo **Rocha** Nunes

RESUMO

O avanço tecnológico e a crescente dependência da Internet e das tecnologias digitais têm impulsionado o desenvolvimento de capacidades cibernéticas em diversas áreas, incluindo a militar. No contexto das Forças Armadas, a cibersegurança tornou-se uma preocupação fundamental, dada a crescente ameaça de ataques cibernéticos a infraestruturas críticas, sistemas de defesa e operações militares. Nesse sentido, a implementação de um Cyber Range para o Exército Brasileiro surge como uma necessidade urgente para preparar suas tropas para enfrentar os desafios cibernéticos do século XXI. Este artigo explora a importância e os benefícios da criação e operação de um Cyber Range eficaz e adaptado às demandas específicas do Exército Brasileiro denominado Simulador de Ações Cibernéticas (SACi) .

Palavras-chave: Cyber Range. Cibernética. Simulador.

Cybernetic Actions Simulator(SACi) Cyber Range of the Brazilian Army preparing the Armed Forces for cyber challenges of the 21st century.

ABSTRACT

Technological advancement and growing dependence on the Internet and digital Technologies have driven the development of cybernetic capabilities in several areas, including the military. In the context of the Armed Forces, cybersecurity has become a key concern, given the growing threat of cyberattacks to critical infrastructure, defense systems, and military operations. In this sense, the implementation of a Cyber Range for the Brazilian Army emerges as an urgent need to prepare its troops to face the cyber challenges of the 21st century. This article explores the importance and benefits of creating and operating an effective Cyber Range, adapted to the specific demands of the Brazilian Army called the Simulator of Cybernetic Actions (SACi).

Keywords: *Electronic Warfare. MAGE NCom. ARP. Radar. Radar Alert.*

Artigo recebido em 31/08/2023 e aceito para publicação em 30/12/2023.

1 INTRODUÇÃO

As guerras do século XXI não serão travadas apenas no campo de batalha físico, mas também nos vastos domínios cibernéticos. A transformação digital trouxe novas oportunidades, mas também aumentou a vulnerabilidade das redes militares a ataques cibernéticos complexos e sofisticados (Avelar, 2018). Nesse contexto, o Exército Brasileiro, responsável pelo setor cibernético das forças armadas, enfrenta o desafio de capacitar suas tropas para defender, atacar e operar no espaço cibernético (Brasil, 2008). Um Cyber Range é uma ferramenta indispensável nessa empreitada, permitindo treinamento em ambientes simulados e realistas.

2 CYBER RANGE E SUA IMPORTÂNCIA

Um Cyber Range é uma infraestrutura de treinamento que simula ambientes cibernéticos realistas, permitindo que as tropas pratiquem suas habilidades de guerra cibernética em condições controladas (KATSANTONIS). Essa abordagem de treinamento oferece uma série de vantagens na preparação das tropas das Forças Armadas.

Soluções de cyber range permitem que profissionais de cibersegurança possam estar preparados para ataques. Longe de nós desmentir o clássico ditado popular de que "a prática leva à perfeição". Quando o assunto é segurança cibernética, a experiência do cotidiano é indispensável e insubstituível para garantir que o profissional do setor saiba lidar com as mais desafiadoras situações de crise. […] (Distrito, 2022)

2.1 REALISMO CONTROLADO

O Cyber Range permite simular cenários complexos e ataques cibernéticos em ambientes seguros e controlados, permitindo aos soldados se familiarizarem com situações reais sem riscos operacionais (NIST).

2.2 TREINAMENTO MULTIDIMENSIONAL

As operações cibernéticas podem ser multifacetadas, envolvendo aspectos técnicos, táticos e estratégicos. O Cyber Range oferece treinamento holístico que abrange diversos níveis de complexidade (NIST).

2.3 AVALIAÇÃO E APERFEIÇOAMENTO CONTÍNUO

Os exercícios no Cyber Range permitem a avaliação do desempenho das tropas, identificando fraquezas e aprimorando habilidades, a fim de fortalecer a resiliência cibernética (NIST).

3 O SIMULADOR DE AÇÕES CIBERNÉTICAS - SACi

O Centro de Instrução de Guerra Cibernética, CIGE, organização militar subordinada ao CCOMGEX, iniciou o desenvolvimento do Simulador de Operações Cibernéticas (SIMOC) 2011, para atender às necessidades do processo de ensino-aprendizagem dos cursos de Guerra Cibernética. Dentre as atribuições de ensino deste Centro, a existência de um ambiente simulado para o ensino das técnicas de ataque, defesa e exploração cibernética, é considerado primordial pelos instrutores do CIGE, tendo em vista que não é viável a utilização de redes em produção, por se tratarem de técnicas que, por vezes, podem comprometer a segurança da informação, dos dados e das comunicações. Sua última atualização ocorreu em 2016, com a inclusão de desafios cibernéticos *capture the flag* no seu código-fonte (CIGE, 2021).

Durante os 10 (dez) anos de utilização do SIMOC, novas capacidades técnicas e procedimentais foram sendo desenvolvidas no ambiente cibernético, o que deixou o simulador descontinuado quanto às principais ações cibernéticas. Ademais, foi observado que o acréscimo de novas funcionalidades sobrecarregaria os processos e poderia extrapolar a sua capacidade de memória, além de ser identificada a incompatibilidade entre os sistemas operacionais que foram instalados na sua última versão, em 2016, e aqueles em uso na atualidade (CIGE, 2021).

Em razão da necessidade de agregar novas funcionalidades e dominar por completo o seu ciclo de vida (CIGE, 2021), a equipe de instrutores e monitores da Seção de Ensino de Guerra Cibernética do CIGE, aproveitando-se do surgimento de novas tecnologias de virtualização e do melhor entendimento acerca dos processos envolvidos em uma simulação cibernética, passou a desenvolver, no ano de 2020, um simulador de ações cibernéticas baseado em tecnologias "open-source", ou seja, com reduzido custo para o Exército Brasileiro, mitigando os problemas que o SIMOC poderia apresentar ao longo do tempo, devido às razões da evolução tecnológica, associada à disponibilidade de recursos de custeio para sua manutenção. Apesar de existirem soluções prontas no mercado, nenhuma delas atendia, plenamente, todas as necessidades do CIGE.

No ano de 2022 foi firmada uma parceria com o Centro de Desenvolvimento de Sistemas, onde aquela OM, reconhecida como uma das Instituições Científicas, Tecnológicas e de Inovação (ICT), passou a dar continuidade ao desenvolvimento do simulador idealizado pelo CIGE sendo assim co-participante da referida invenção (CDS, 2022).

Ainda, naquele ano, visualizou-se parceria com o Instituto Militar de Engenharia ao qual viabilizou a participação de 1 aluno e 1 professor de Engenharia de Software durante 12 meses para o apoio no projeto. A previsão de entrega para o ano de 2023 dos módulos de INSTRUTOR, que permitirá a criação de cenários e organização dos ambientes cibernéticos e do módulo ALUNO, o qual permitirá o acesso ao ambiente controlado, além de contar com o módulo de VPN, o qual permitirá o aluno entrar no ambiente controlado a partir de sua própria máquina (2°CGEO, 2022).

3.1 TECNOLOGIA DESENVOLVIDA

O Simulador de Ações Cibernéticas (SACi) é um sistema de aplicação didática empregado em cursos de capacitação, especialização e extensão que exijam do aluno conhecimentos técnicos na operação de recursos de tecnologia da informação e comunicações em um ambiente de operações cibernéticas no âmbito das Forças Armadas (FA).

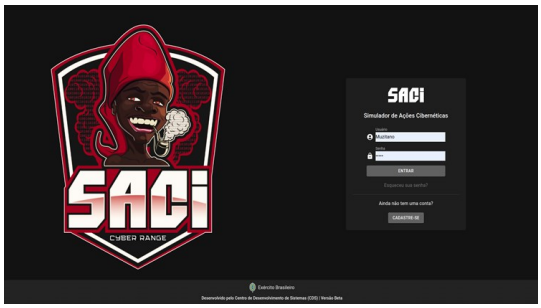
O simulador virtualiza o comportamento de uma rede típica, composta de roteadores, switches, firewalls e estações de trabalho. Além disso,

também simula serviços de rede, tais como servidor de correio eletrônico, servidor de páginas (servidor Web), servidor de arquivos, além de simular enlaces de dados, perfis de tráfego de redes, dentre outros serviços de rede existentes no mundo real. As ações desencadeadas pelos alunos têm reflexo no comportamento do ambiente de simulação, a partir de condições e cenários pré-definidos pelos instrutores, de modo que, por meio do emprego de técnicas de virtualização, é capaz de implementar um ambiente estanque no qual os alunos podem conduzir e reproduzir, de forma segura e controlada, ações e situações encontradas no mundo cibernético real.

A página web do SACi serve como uma ferramenta de Área de Trabalho Remota, pois permite conexão SSH, VNC e RDP. Ele funciona como um *gateway* de Desktop Remoto que só precisa ser instalado em um servidor central. Assim, ele fornecerá um painel de controle, baseado na web, que lhe permitirá mudar rapidamente de uma máquina para outra – tudo dentro da mesma janela do navegador.

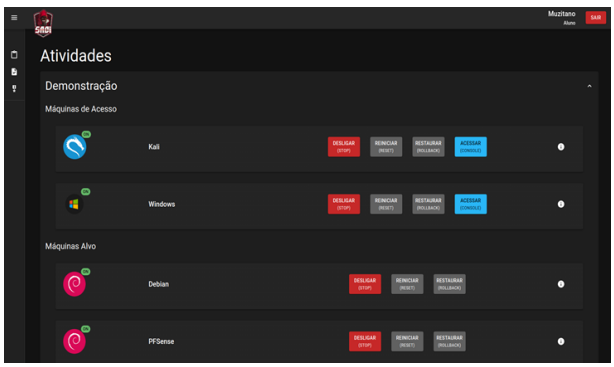
A página de *login* encontra-se na Figura 1:

Figura 1 – Tela Login



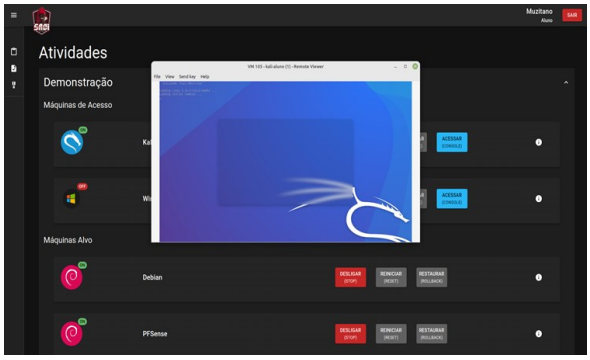
Após realizar o login o aluno é levado a sua própria página onde terá acesso aos ativos que foram virtualizados para seu treinamento, como demonstrado na Figura 2:

Figura 2 – Tela Atividades



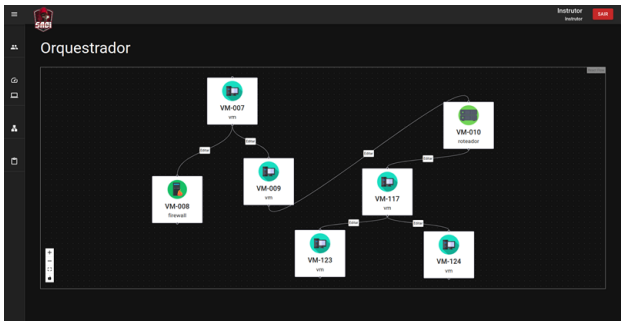
Na Figura 3 imagem podemos ver uma interação do usuário com sua máquina:

Figura 3 – Tela com interação do usuário



Na Figura 4 é possível ver o mapa de rede que é disponibilizado para o aluno, onde através do orquestrador ele tem uma visão mais ampla de sua rede pessoal.

Figura 4 – Mapa da rede



3.2 MÓDULOS

A intenção de se criar em código aberto é a facilidade de novas ideias serem agregadas a plataforma central do SACi, assim já estão sendo desenvolvidos outros módulos como os de CAPTURE THE FLAG, VPN, INFRAESTRUTURAS CRÍTICAS, INTELIGÊNCIA ARTIFICIAL, DEMONSTRAÇÃO DE ATAQUES CIBERNÉTICOS e fomentados por alunos do IME em seus trabalhos de conclusão de curso e dissertação de mestrado, como nos artigos científicos do curso de Guerra Cibernética no CIGE.

Figura 5 – Módulo de infraestruturas

4 BENEFÍCIOS DO SACI PARA O EXÉRCITO BRASILEIRO

A implementação do Simulador de Ações Cibernética (SACi) no Exército Brasileiro oferece uma série de benefícios que impactam positivamente suas operações. A customização é uma das vantagens mais notáveis, pois permite adaptar as funcionalidades do simulador de acordo com as necessidades específicas da Força Terrestre. Com isso, o SACi pode ser ajustado para refletir as políticas, Técnicas, Táticas e Procedimentos (TTP) que serão empregados em suas operações de ciberdefesa.

Além disso, a adoção do SACi apresenta uma solução econômica e escalável para o Exército Brasileiro. Ao contrário da contratação de serviços de terceiros, que pode ser dispendiosa e limitada em termos de flexibilidade, o SACi oferece maior controle sobre o processo de desenvolvimento, teste e implementação. Isso permite ao Exército ter total domínio sobre os dados utilizados, as configurações de simulação e as métricas de desempenho, garantindo a eficácia e a eficiência dos treinamentos.

O SACi também é uma ferramenta eficaz para o treinamento das equipes de exploração, ataque e proteção cibernética. Os membros da equipe podem praticar e aprimorar suas habilidades em um ambiente simulado e seguro, sem expor a Força a riscos desnecessários.

Além disso, a experiência de simulação pode ser personalizada para atender às necessidades individuais de cada membro da Organização Militar (OM), proporcionando um treinamento mais eficiente e ágil.

Outro ponto relevante é que o desenvolvimento do SACi pode estimular a inovação e o pensamento criativo das equipes envolvidas na ciberdefesa. O ambiente simulado permite que as equipes experimentem novas abordagens e testem novas tecnologias antes de aplicá-las em cenários reais, impulsionando a busca por soluções mais avançadas e eficazes.

Outra capacidade fundamental do SACi é a simulação de diferentes cenários de ameaças e a testagem de respostas diversas. Isso resulta em uma tomada de decisão mais informada e embasada, preparando a equipe para lidar com situações reais de ameaça cibernética com maior precisão e efetividade.

Além dos benefícios operacionais, a implementação do SACi também fomenta a colaboração. Nesse contexto, o Instituto Militar de Engenharia (IME), o Centro de Desenvolvimento de Sistema (CDS) e o Comando de Comunicações e Guerra Eletrônica do Exército (CCOMGEX), através do CIGE, trabalham em conjunto para a produção de novos conhecimentos, a promoção da inovação tecnológica e o desenvolvimento no âmbito da ciberdefesa.

5 CONCLUSÃO

A cibersegurança é uma prioridade estratégica para o Exército, e a preparação para os desafios cibernéticos requer uma abordagem holística que inclua o treinamento adequado das tropas.

A implementação de um Cyber Range dedicado ao Exército é uma iniciativa essencial para aprimorar as capacidades cibernéticas e garantir a prontidão para enfrentar as ameaças cibernéticas emergentes. Com investimentos nessa área, o Exército estará melhor preparado para proteger suas redes, defender suas operações e manter a superioridade cibernética nas futuras batalhas. Assim, a implementação do Simulador de Ações Cibernética (SACi) traz uma série de benefícios cruciais para a ciberdefesa do país.

A customização, economia de recursos, controle do processo de desenvolvimento, eficiência no treinamento da equipe, incentivo à inovação, simulação de cenários e a colaboração representam vantagens significativas.

O SACi emerge como uma ferramenta estratégica e imprescindível para fortalecer a cibersegurança e a preparação das Forças Armadas diante dos desafios cada vez mais complexos e dinâmicos do cenário cibernético.

REFERÊNCIAS BIBLIOGRÁFICAS

AVELAR, José Ricardo Cabral. Guerra Cibernética e seus desafios para o Brasil. 2018. 74f. **Trabalho de Conclusão de Curso** (Especialização em Ciências Militares) - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2018. Disponível em: https:// bdex.eb.mil.br/jspui/ bitstream/123456789/2893/1/MO%205894%20-%20AVELAR.pdf. Acesso em: 04 set. 2023.

BRASIL. Centro de Instrução de Guerra Eletrônica (CIGE). **Projeto SACi**, 11 de outubro 2022. Brasília, 2022.

BRASIL. Decreto nº 6.703, de 18 de dezembro de 2008. **Aprova a Estratégia Nacional de Defesa**. Brasília, 2008.

BRASIL. Centro de Instrução de Guerra Eletrônica (CIGE). Justificativa para a devolução do recurso e mudança do objeto da licitação do SIMOC. **Memória de Decisão** nº 001/CIGE, 23 de setembro de 2021. Brasília, 2021.

DISTRITO. **Cyber range**: plataforma e solução de simulação de ataques, 3 de março de 2022. Disponível em: https://distrito.me/blog/o-que-e-cyber-range/. Acesso em: 04 ago. 2023.

KATSANTONIS, M. N.; MANIKAS, A.; MAVRIDIS, I.; GRITZALIS, D. Cyber range design framework for cyber security education and training. **International Journal of Information Security**, v. 22, p. 1005-1027, 2023. Disponível em: https://link.springer.com/article/10.1007/s10207-023-00680-4#Sec1. Acesso em: 04 set. 2023.

NIST. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. The Cyber Range: A Guide. Disponível em: https://www.nist.gov/system/files/documents/2020/06/25/The%20Cyber%20Range%20-%20A%20Guide%20%28NIST-NICE%29%20%28Draft%29%20-%20062420_1315.pdf. Acesso em: 10 ago. 2023.