Cibersegurança com autonomia: como a RNP capacita o Brasil com simulações de ataque e defesa

Rildo A. Souza[1], **Davi D. Gemmer**[2]

[1]Rede Nacional de Ensino e Pesquisa(RNP)
13086-902 – Campinas – SP – Brasil

rildo.souza@rnp.br, davi.gemmer@rnp.br

Resumo. *Este trabalho apresenta o RNP CiberRange, uma plataforma voltada à capacitação prática em cibersegurança por meio de simulações de ataque e defesa em ambientes controlados. O artigo analisa a iniciativa a partir de referenciais sobre resiliência cibernética, cyber ranges, emulação adversária e breach and attack simulation, situando a solução no contexto da formação técnica e da experimentação aplicada. Também são descritas características da plataforma, como virtualização, modelagem flexível de cenários, automação de eventos e dinâmicas colaborativas e competitivas. Como contribuição, o trabalho evidencia o potencial do RNP CiberRange para ampliar o acesso a treinamentos práticos, apoiar a formação especializada e fortalecer capacidades nacionais em cibersegurança.*

1. Introdução

O cenário contemporâneo de ameaças cibernéticas tem impulsionado a necessidade de abordagens que não se limitem à prevenção, mas que também contemplem preparação, resistência, recuperação e adaptação diante de eventos adversos.

Nesse contexto, destaca-se inicialmente o *National Institute of Standards and Technology* (NIST), órgão do governo dos Estados Unidos amplamente reconhecido pela produção de normas, guias e referências técnicas em segurança da informação e cibersegurança. A partir de suas publicações, a resiliência cibernética é compreendida como parte de uma abordagem de engenharia de sistemas seguros e confiáveis, associada a objetivos, técnicas e princípios de projeto voltados ao enfrentamento de ameaças cibernéticas e não cibernéticas ao longo do ciclo de vida dos sistemas [National Institute of Standards and Technology (NIST) 2021]. Sob essa perspectiva, a crescente complexidade do cenário de ameaças amplia a necessidade de abordagens que não se limitem à prevenção, mas que também contemplem preparação, resistência, recuperação e adaptação diante de eventos adversos. Essa visão amplia o foco tradicional da segurança da informação ao reconhecer que a proteção efetiva depende da articulação entre tecnologia, processos organizacionais e capacidades humanas [National Institute of Standards and Technology (NIST) 2021].

Em paralelo, a *MITRE Corporation* destaca-se por contribuições metodológicas relevantes para a área, especialmente por meio do ATT&CK, base de conhecimento amplamente utilizada para descrever táticas, técnicas e procedimentos (*Tactics, Techniques and Procedures* – TTPs) empregados por agentes de ameaça em cenários reais. Nesse contexto, os *Adversary Emulation Plans* demonstram a aplicação prática desse referencial por equipes ofensivas e defensivas, permitindo testar redes e mecanismos de proteção

com base em relatórios públicos de ameaças e na modelagem de comportamentos adversários [MITRE ATT&CK 2026]. Tal abordagem favorece a avaliação de ambientes, controles e capacidades analíticas a partir de comportamentos observáveis, em vez de se restringir a indicadores específicos de comprometimento ou ao uso isolado de ferramentas [MITRE ATT&CK 2024]. Assim, a emulação adversária se consolida como abordagem relevante para tornar os exercícios de segurança mais aderentes às ameaças observadas na prática [MITRE ATT&CK 2024].

O conjunto de normas, táticas e técnicas utilizadas por usuários maliciosos e evidenciados por esses órgãos tornam necessário a utilização de ambientes de simulação reais para testes e aprendizagem. Nesse contexto o RNP CiberRange consiste em um sistema virtualizado que visa promover simulações de ataque e defesa cibernética e, portanto, a formação prática de profissionais e equipes. O sistema permite criar cenários de forma realista e realizar treinamentos baseados em jogos, incluindo *Wargame*, competições do tipo *Capture The Flag* (CTF) e *C*yber Knowledge Check (CKC). Os dois primeiros são atividades de formação competitiva, enquanto os CKCs permitem avaliar o conhecimento dos participantes sobre cibersegurança. Todos esses treinamentos podem ser realizados sem necessidade de infraestrutura adicional por parte do usuário.

2. Referencial Teórico

Um ator relevante no contexto de cibersegurança é a *Cybersecurity and Infrastructure Security Agency* (CISA), agência do governo dos Estados Unidos voltada à proteção de infraestrutura crítica e ao fortalecimento da segurança cibernética. A CISA contribui para essa discussão ao divulgar materiais e iniciativas de capacitação técnica voltados ao treinamento prático em ambientes simulados. Em suas iniciativas de treinamento, a agência descreve atividades em ambientes virtuais realistas e laboratoriais voltadas ao desenvolvimento de capacidades operacionais, reforçando o valor dos *cyber ranges* como infraestrutura de aprendizagem aplicada [Cybersecurity and Infrastructure Security Agency (CISA) 2024].

Nesse panorama, as plataformas de *Breach and Attack Simulation* (BAS) também podem ser compreendidas como expressão prática da validação contínua de controles de segurança, ao automatizarem a execução segura de cenários ofensivos em ambientes corporativos. De modo geral, essas soluções buscam simular comportamentos adversários realistas para identificar lacunas de detecção, falhas de configuração, limitações de cobertura e oportunidades de melhoria na resposta defensiva [National Institute of Standards and Technology (NIST) 2024]. No mercado internacional, fornecedores como SafeBreach, Picus Security, Cymulate, XM Cyber e AttackIQ ilustram a consolidação desse segmento, com ofertas voltadas à validação contínua da postura de segurança, à simulação automatizada de ataques e à priorização de exposições com base em caminhos de ataque e efetividade dos controles.

A SafeBreach apresenta sua plataforma como uma solução de validação de exposição que combina capacidades de BAS com validação de caminhos de ataque, buscando identificar falhas de controles e demonstrar o que um atacante poderia alcançar ao explorá-las [SafeBreach 2026]. A Picus Security define BAS como um método automatizado e contínuo para testar defesas por meio da simulação segura de ataques reais em ambiente controlado, com ênfase na identificação de pontos cegos, falhas silenciosas e la-

cunas de política [Picus Security 2026]. De forma semelhante, a Cymulate descreve sua plataforma como mecanismo para automatizar cenários de ataque do mundo real, avaliar a postura de segurança e validar defesas contra ameaças ativas [Cymulate 2026]. Já a XM Cyber enfatiza a validação de exposições e caminhos de ataque em uma perspectiva de *continuous exposure management*, aproximando o BAS de modelos mais amplos de gestão contínua da superfície de risco [XM Cyber 2026]. A AttackIQ, por sua vez, associa BAS à validação das defesas com cenários reais e à melhoria contínua da efetividade do programa de segurança [AttackIQ 2026].

Além dessas plataformas, há soluções correlatas que dialogam com o mesmo espaço tecnológico, ainda que com ênfases distintas. A CyCognito, por exemplo, posiciona-se em torno de *adversarial exposure validation*, com foco em descoberta e teste contínuo da superfície de ataque externa [CyCognito 2026]. A Circadence, por sua vez, concentra sua atuação em ambientes de *cyber range* de alta fidelidade e em infraestrutura para treinamento e exercícios técnicos, aproximando-se do campo de simulação aplicada e capacitação operacional [Circadence 2026]. Esses exemplos demonstram que o ecossistema internacional reúne tanto plataformas BAS em sentido estrito quanto soluções adjacentes de validação adversária, emulação e ambientes de treinamento.

Observa-se, que as soluções mais visíveis e consolidadas nesse segmento são predominantemente estrangeiras. Entre os exemplos destacados, encontram-se empresas sediadas fora do Brasil, em especial nos Estados Unidos e em outros polos internacionais de cibersegurança. Esse aspecto é relevante porque sugere uma dependência tecnológica de plataformas externas para atividades estratégicas de validação contínua, simulação de ataques e desenvolvimento de capacidades operacionais. Nesse sentido, a proposição de uma alternativa brasileira adquire importância não apenas do ponto de vista técnico, mas também científico, econômico e institucional, ao contribuir para a formação de conhecimento local, para a adaptação a contextos nacionais de ensino e operação e para a redução da dependência de soluções estrangeiras em uma área sensível da cibersegurança.

Nesse sentido, a plataforma em desenvolvimento contribui diretamente para o propósito da RNP, ao integrar formação prática, experimentação aplicada e aprimoramento técnico em cibersegurança. Ao articular resiliência cibernética, exercícios adversariais, simulação de ataques e ambientes controlados de aprendizagem, a solução apoia tanto o desenvolvimento de competências profissionais quanto a produção de conhecimento, reforçando a atuação da RNP na promoção de iniciativas que conectam ensino, pesquisa, inovação e capacitação técnica.

3. RNP CiberRange

O RNP CiberRange é uma ferramenta de aprendizagem que visa fornecer treinamento prático em cibersegurança, criado para auxiliar nas simulações de ataques e defesas dentro de um ambiente com Tecnologias de Informações e Comunicação (TIC). O CiberRange faz parte do cenário dos *cyber ranges*, sendo um ambiente protegido e controlado que permite a realização de simulações reais, o que auxilia na obtenção de habilidades operacionais e no encaminhamento entre teoria e prática na cibersegurança [National Institute of Standards and Technology (NIST) 2023].

A fim de atender a esse propósito, o sistema foi desenvolvido de maneira a permitir a realização de treinamentos através da simulação de cenários que possam retratar uma

situação real de ameaças, incluindo simulações de incidentes, testes controlados de vulnerabilidades, análise de incidentes de segurança e defesa e exercícios especializados. Isso se alinha às abordagens atuais de treinamento na área de cibersegurança, onde há ênfase no uso de um ambiente simulado para capacitação técnica e habilidades de operações [Cybersecurity and Infrastructure Security Agency (CISA) 2026].

O sistema usa uma interface Web para desenvolver, configurar e executar os cenários, facilitando a realização da atividade de forma remota e minimizando os obstáculos técnicos e físicos existentes que dificultam a participação no processo. O sistema monta um ambiente caracterizado por ser hiper-realístico, baseado na virtualização e capaz de simular redes, serviços, equipamentos e elementos de segurança com diversas configurações de treinamento. Além disso, pode ser aplicada a automatização dos eventos, catalogação de objetos, usuários diferenciados e módulos especiais para aprendizado competitivo.

Esse modelo dialoga com a noção de *mitre* difundida pela MITRE, segundo a qual exercícios mais efetivos devem se apoiar em comportamentos adversários observáveis e em estruturas que permitam testar redes e controles defensivos de forma mais aderente à realidade. Nesse sentido, ambientes como o RNP CiberRange podem funcionar não apenas como laboratórios didáticos, mas também como instrumentos de validação técnica, experimentação e amadurecimento operacional [MITRE ATT&CK 2026].

A flexibilidade da plataforma também é demonstrada através de simulação no design dos ambientes de treinamento. Os ambientes poderão ser criados por meio de interface Web de acordo com os requisitos pedagógicos e operacionais de cada atividade, utilizando tanto como suporte de visualizações na criação, quanto a estruturação do ambiente em YAML. Essa criação será facilitada pela existência de um conjunto de objetos, compostos por recursos e máquinas virtuais pré-configurados, possibilitando a expansão da quantidade de recursos que podem ser utilizados na construção dos ambientes e contribuindo para melhor integração com as ferramentas de segurança utilizadas na prática. Ademais, a literatura sobre *cyber ranges* aponta que a relevância desses ambientes reside fortemente no fato de que a capacidade de construir e combinar cenários de maneira flexível é fundamental para seu desempenho [Yamin et al. 2020].

Em termos didático operacionais, os treinamentos podem ocorrer tanto no formato de cenários compartilhados, quanto no formato de cenário individualizado, sendo possível realizar treinamentos coletivos e competitivos, inclusive no estilo *red teams* versus *blue teams*. Neste cenário, é possível delinear tarefas específicas para auxiliar na atuação das equipes, bem como as funções que possam modificar a atuação deste ambiente ao decorrer do treinamento. As funções podem ocorrer de maneira automática, mediante certas condições pré determinadas, ou então de forma manual, conforme o desenrolar da simulação, tornando os treinamentos mais dinâmicos e alinhados à capacitação técnica. Esse conjunto de funcionalidades e personalizações foi observado em diferentes simuladores reforçando que tais recursos são reconhecidos como elementos relevantes para a condução de treinamentos mais completos [Yamin and Katt 2022].

O que contribui para posicionar o RNP CiberRange como uma iniciativa com potencial para ampliar o acesso a treinamentos práticos, apoiar a formação especializada e fortalecer a autonomia nacional na produção de capacidades em cibersegurança.

4. Conclusão

O estudo em questão destacou a criação de um simulador de cibersegurança denominado CiberRange RNP como sendo uma ferramenta de formação profissional. Diante da análise feita sobre os fundamentos teóricos aqui aplicados, percebeu-se que a utilização de *cyber ranges* podem ser vistas como estratégias válidas para a formação dos profissionais na prática operacional.

Para o caso sob estudo, o RNP CiberRange é um exemplo de implementação das metodologias citadas no âmbito nacional, ao unir técnicas de simulação, virtualização e gamificação em prol do desenvolvimento e da prática. Desta forma, esta ferramenta auxilia na minimização da diferença entre o que se aprende teoricamente e a prática da defesa cibernética.

Ademais, a pesquisa demonstra a importância de medidas implementadas na esfera nacional, direcionadas à especialização de profissionais no campo da cibersegurança, levando em consideração o domínio das ferramentas desenvolvidas internacionalmente. No entanto, a plataforma RNP CiberRange pode ser utilizada como um importante facilitador desses processos de capacitação.

Como perspectiva futura, destaca-se a importância de avaliar empiricamente os impactos educacionais e operacionais da plataforma, considerando aspectos como efetividade do aprendizado, desenvolvimento de competências e aplicabilidade e evolução dos cenários em diferentes contextos de capacitação.

Declaração de uso de IA

Os autores declaram que utilizaram a ferramenta ChatGPT, da OpenAI, exclusivamente para apoio à revisão textual, melhoria de clareza, fluidez e correção gramatical do manuscrito. A ferramenta não foi utilizada para geração de resultados, análise de dados, elaboração de conclusões ou produção de conteúdo científico original. Todo o conteúdo final foi revisado, validado e é de responsabilidade dos autores.

Referências

AttackIQ (2026). Breach and attack simulation. Disponível em: `https://www.attackiq.com/glossary/breach-and-attack-simulation/`. Acesso em: 2 abr. 2026.

Circadence (2026). Range design and engineering. Disponível em: `https://circadence.com/range-design-engineering/`. Acesso em: 2 abr. 2026.

Cybersecurity and Infrastructure Security Agency (CISA) (2024). Cybersecurity education and career development. Disponível em: `https://www.cisa.gov/resources-tools/programs/cybersecurity-education-career-development`. Acesso em: 25 mar. 2026.

Cybersecurity and Infrastructure Security Agency (CISA) (2026). Cybersecurity training and exercises. Disponível em: `https://www.cisa.gov/resources-tools/training`. Acesso em: 25 mar. 2026.

CyCognito (2026). Understanding adversarial exposure validation. Disponível em: https://www.cycognito.com/learn/exposure-management/adversarial-exposure-validation/. Acesso em: 2 abr. 2026.

Cymulate (2026). What is breach and attack simulation (BAS)? Disponível em: https://cymulate.com/breach-and-attack-simulation/. Acesso em: 2 abr. 2026.

MITRE ATT&CK (2024). Adversary emulation and red teaming. Acesso em: 25 mar. 2026.

MITRE ATT&CK (2026). Adversary emulation plans. Disponível em: https://attack.mitre.org/resources/adversary-emulation-plans/. Acesso em: 25 mar. 2026.

National Institute of Standards and Technology (NIST) (2021). SP 800-160 Vol. 2 Rev. 1: Developing cyber-resilient systems: A systems security engineering approach. Disponível em: https://doi.org/10.6028/NIST.SP.800-160v2r1. Acesso em: 25 mar. 2026.

National Institute of Standards and Technology (NIST) (2023). The cyber range: A guide. Disponível em: https://www.nist.gov/document/cyber-range. Acesso em: 25 mar. 2026.

National Institute of Standards and Technology (NIST) (2024). Red team exercise. Computer Security Resource Center Glossary. Disponível em: https://csrc.nist.gov/glossary/term/red_team_exercise. Acesso em: 25 mar. 2026.

Picus Security (2026). Breach and attack simulation platform. Disponível em: https://www.picussecurity.com/platform/breach-and-attack-simulation. Acesso em: 2 abr. 2026.

SafeBreach (2026). Exposure validation platform. Disponível em: https://www.safebreach.com/safebreach-exposure-validation-platform/. Acesso em: 2 abr. 2026.

XM Cyber (2026). Continuous exposure management platform. Disponível em: https://xmcyber.com/platform/. Acesso em: 2 abr. 2026.

Yamin, M. M. and Katt, B. (2022). Use of cyber attack and defense agents in cyber ranges: A case study. *Computers & Security*, 122:102892.

Yamin, M. M., Katt, B., and Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, 88:101636.