DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Identificação de Competências dos *Cyber Red Teams* Militares e Proposta de Metodologia de Treinamento Contínuo para Projeção do Poder na Guerra Cibernética

José Augusto de Almeida Junior

Brasília, Agosto de 2020

Programa de Pós-Graduação Profissional em Engenharia Elétrica
DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

Identification Of Military Cyber Red Teams Skills And Proposed Continuous Training Methodology For Projecting Power In Cyber Warfare

Identificação de Competências dos *Cyber Red Teams* Militares e Proposta de Metodologia de Treinamento Contínuo para Projeção do Poder na Guerra Cibernética

JOSÉ AUGUSTO DE ALMEIDA JUNIOR

ORIENTADOR: WILLIAM FERREIRA GIOZZA, DR.
COORIENTADOR: ROBSON DE O. ALBUQUERQUE, DR.

DISSERTAÇÃO DE MESTRADO PROFISSIONAL EM
ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPEE.MP.003
BRASÍLIA/DF: AGOSTO - 2020

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Identificação de Competências dos *Cyber Red Teams* Militares e Proposta de Metodologia de Treinamento Contínuo para Projeção do Poder na Guerra Cibernética

José Augusto de Almeida Junior

Dissertação de mestrado profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Prof. Robson de O. Albuquerque, Ph.D, FT/UnB _____
Orientador

Prof. Rafael Timóteo de Sousa Júnior, Ph.D, FT/UnB _____
examinador interno

Prof. André Ricardo Abed Grégio, Ph.D, UFPR _____
Examinador externo

Prof. Rafael Rabelo Nunes, Ph.D, FT/UnB _____
Suplente

FICHA CATALOGRÁFICA

DE ALMEIDA JUNIOR, JOSÉ AUGUSTO
Identificação de Competências dos *Cyber Red Teams* Militarese Proposta de Metodologia de Treinamento Contínuo para Projeção do Poder na Guerra Cibernética [Distrito Federal] 2020.
xvi, 64 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2020).
Dissertação de mestrado profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Guerra cibernética
2. Cyber red team
3. Projeção de poder militar
4. Treinamento

REFERÊNCIA BIBLIOGRÁFICA

DE ALMEIDA JR., J.A. (2020). *Identificação de Competências dos Cyber Red Teams Militarese Proposta de Metodologia de Treinamento Contínuo para Projeção do Poder na Guerra Cibernética*. Dissertação de mestrado profissional, Publicação: PPEE.MP.003, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 64 p.

CESSÃO DE DIREITOS

AUTOR: José Augusto de Almeida Junior
TÍTULO: Identificação de Competências dos *Cyber Red Teams* Militarese Proposta de Metodologia de Treinamento Contínuo para Projeção do Poder na Guerra Cibernética.
GRAU: Mestre em Engenharia Elétrica ANO: 2020

José Augusto de Almeida Junior
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico esse trabalho a Deus, por permitir que esse sonho se concluísse e a minha família, amigos e namorada, por todo apoio nesse momento de minha vida. Dedico também aos meus chefes e colegas de trabalho, por colaborarem grandemente com esse feito.

“As pessoas costumam dizer que a motivação não dura sempre. Bem, nem o efeito do banho, por isso recomenda-se diariamente.”

(Zig Ziglar)

AGRADECIMENTOS

A Deus por ter permitido minha saúde e força de vontade para superar as dificuldades. A Universidade de Brasília, a Faculdade de Tecnologia, ao corpo docente, direção, administração e a secretaria que deram grande apoio e oportunizaram esse novo horizonte ao qual vislumbro. Agradeço aos meus chefes por permitirem a minha participação neste programa de mestrado e a todos os colegas de trabalho que colaboraram diretamente. A minha família, a minha namorada e aos meus amigos, que incentivaram e colaboraram durante esse período. Um agradecimento especial ao meu orientador Prof. Dr. William Ferreira Giozza e ao meu coorientador Prof. Dr. Robson de Oliveira Albuquerque, que realizaram um excelente trabalho de orientação, ao qual devo o sucesso desta dissertação. A todas as pessoas que direta ou indiretamente fizeram parte da minha formação, meus sinceros agradecimentos.

RESUMO

Título: Identificação de Competências dos *Cyber Red Teams* Militares e Proposta de Metodologia de Treinamento Contínuo para Projeção do Poder na Guerra Cibernética
Autor: José Augusto de Almeida Junior
Orientador: William Ferreira Giozza, Dr.
Coorientador: Robson de O. Albuquerque, Dr.
Programa de Pós-Graduação Profissional em Engenharia Elétrica
Brasília, 3 de agosto de 2020

Defesa, reconhecimento e ataque são pré-requisitos para a projeção do poder militar na guerra cibernética e a eficácia das forças armadas nessas atividades determinam a imposição do Estado no mundo contemporâneo. Para melhorar suas habilidades cibernéticas, as organizações militares, geralmente, criam exercícios para suas equipes ofensivas e defensivas. Esses exercícios aumentam as habilidades cibernéticas, mas são periódicos e dependem da disponibilidade de profissionais. Para além disso, nota-se também que existe uma grande dificuldade, principalmente pelos Estados menos desenvolvidos, de estabelecer as habilidades necessárias a serem buscadas para suas equipes ofensivas. Isso acontece, pois determinados nichos como no caso das organizações militares possuem certas peculiaridades que precisam ser bem compreendidas antes da implantação de um *cyber red team*. Neste trabalho são identificadas as competências que um *cyber red team* deve ter no contexto militar. Foram identificadas quatro competências macro, de onde se originaram mais oito competências, a partir das suas intersecções sucessivas. Com isso, pretende-se apresentar uma visão mais clara das competências necessárias para um *cyber red team* militar, de forma a aumentar a eficiência de sua montagem e ação nesse contexto. Para esse fim, este trabalho propõe também uma metodologia de treinamento contínuo que não exige que os profissionais se envolvam exclusivamente nos exercícios, mas que permite um aumento constante das habilidades cibernéticas. Essa metodologia proposta trabalha com três redes diferentes em paralelo. Uma rede exclusiva para desenvolvimento de ataques, outra para confronto real em ambiente simulado e a rede de produção, que sofre correções de acordo com as falhas encontradas no confronto simulado. Para eficácia dessa metodologia proposta, leva-se em consideração que existem três equipes, o *cyber red team* para ações ofensivas, o *cyber blue team* para ações defensivas e o *cyber purple team* que é responsável por gerenciar as infraestruturas das redes propostas na metodologia. A eficácia da metodologia foi demonstrada a partir de um experimento de aproximadamente nove meses que foi realizado com a participação de dezessete militares. Neste experimento foi constatado o aprimoramento das habilidades inerentes aos pré-requisitos para a projeção do poder militar na guerra cibernética, sem causar danos à atividade real.

Palavras-chave: Guerra cibernética, *Cyber red team*, Projeção de poder militar, Treinamento.

ABSTRACT

Title: Identification Of Military Cyber Red Teams Skills And Proposed Continuous Training Methodology For Projecting Power In Cyber Warfare
Author: José Augusto de Almeida Junior
Supervisor: William Ferreira Giozza, Dr.
Co-Supervisor: Robson de O. Albuquerque, Dr.
Professional Post-Graduate Program in Electrical Engineering
Brasília, August 3, 2020

Defense, reconnaissance and attack are prerequisites for the military power projection when considering cyber warfare, also the effectiveness of the armed forces in these activities determines the imposition of the its States in the contemporary world. In order to improve cyber skills of their personnel, military organizations often create exercises to put to the test cyber red and blue teams. Such exercises increase their cyber skills, but they are periodic and high dependent on the availability of professionals. In addition, it is also noted that there is a great difficulty, mainly by the less developed States to establish the necessary skills to be sought for their offensive teams. This happens because certain niches as in the case of military organizations have peculiarities that must be well understood before to implement a cyber red team. This work identifies the competencies required for a cyber red team in the military context. Four macro competences were specified, originating by their successive intersections eight more competences. In this context, we expect to provide a better vision of the skills needed for a military cyber red team, in order to increase the efficiency of its composition and action in this context. With such considerations in mind, this work proposes a cyber red team formation methodology with continuous training that does not require professionals to be exclusively involved in the exercises, but which permits a constant development of cyber skills. The proposed methodology also considers different knowledge domains with three different networks in parallel. An exclusive network for cyber attacks developments, another for attack and defense teams confrontation in a simulated environment and the production network, which is corrected according to the flaws found in the simulated confrontation. For the effectiveness of the proposed methodology, there must be three cyber teams, the cyber red team for offensive actions, the cyber blue team for defensive actions and the cyber purple team, which acts as judge and manages the infrastructures of the networks proposed in the methodology. Methodology effectiveness was demonstrated from an experiment of nine months approximately that was carried out with the participation of seventeen militaries. In this experiment, the skills inherent in prerequisites for the military power projection in cyber warfare inhanced and there was not causing real damage to cyber production environments.

Keywords: Cyber warfare, Cyber red team, Military power projection, Training.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÔNIMOS

Siglas

AISTI	Associação Ibérica de Sistemas e Tecnologias de Informação
CTF	*Capture The Flag* (Captura da Bandeira)
CYOP	*Cyber Psychological Operations* (Operações Ciber-Psicológicas)
DDoS	*Distributed Denial of Service* (Negação de Serviço de Distribuída)
DNS	*Domain Name System* (Sistema de Nomes de Domínios)
EA	Efetividade do Ataque
EUA	Estados Unidos da América
ICITS'20	Conferência Internacional Tecnologia da Informação e Sistemas de 2020
IDS	*Intrusion Detection System* (Sistema de Detecção de Intrusos)
IoT	*Internet of Things* (Internet das Coisas)
IPS	*intrusion Prevent System* (Sistema de Prevenção de Intrusão)
ISSAF	*Information Systems Security Assessment Framework* (Estrutura de Avaliação de Segurança do Sistema de Informação)
ISSN	*International Standard Serial Number* (Número Internacional Normalizado para Publicações Seriadas)
NSA	*National Security Agency* (Agência de Segurança Nacional dos Estados Unidos)
OSINT	*Open Source Intelligence* (Inteligência de Fontes Abertas)
OSSINT	*Open Source Social Network Intelligence* (Inteligência de Fontes Abertas em Redes Sociais)
OSSTMM	*Open Source Security Testing Methodology Manual* (Manual Metodologico de Teste de Segurança de Código Aberto)
OTAN	Organização do Tratado do Atlântico Norte
OWASP	*Open Web Application Security Project* (Projeto Aberto de Segurança em Aplicações Web)
PTES	*Penetration Testing Execution Standard* (Padrão de Execução de Teste de Penetração)
RISTI	Revista Ibérica de Sistemas e Tecnologias de Informação
SBC	*Single-Board Computer* (Computador de Placa Única)
SCADA	*Supervisory Control and Data Acquisition* (Controle Supervisório e Aquisição de Dados)
URL	*Uniform Resource Locator* (Localizador Padrão de Recursos)
WAF	*Web Application Firewall* (Firewall de Aplicações Web)
TTP	Tática, Técnica e Procedimento

IP	*Internet Protocol* (Protocolo de Internet)
WWW	*world wide web* (Rede Mundial de Computadores)
SQL	*Standard Query Language* (Linguagem de Consulta Estruturada)
TCD	Tempo de Cálculo de Danos
TDA	Tempo de Desenvolvimento de Ataques
TIA	Tempo de Identificação do Ataque
TIC	Tecnologia de Informação e Comunicação
TID	Tempo de Implementação da Defesa
TOA	Tempo de Ocultação do Ataque
TTD	Tempo Total para Defesa

1 INTRODUÇÃO

Com a crescente da internet, manter a segurança da informação tornou-se um grande problema, principalmente para as forças armadas que são obrigadas a trabalhar o ambiente virtual como um ambiente de guerra [1]. As empresas desenvolvedoras de *softwares* lançam, com frequência, *patches* de correção para vulnerabilidades, no entanto isso não impede que as organizações sejam afetadas por ataques cibernéticos, já que isso depende de diversos outros fatores [2].

Quando falamos em defesa de um Estado, o controle dos ativos, vulnerabilidades e ameaças tornam-se essenciais para as forças armadas, já que podem ser consideradas a linha de defesa de seu Estado [3]. Caso um ataque cibernético atinja com sucesso, por exemplo, as infraestruturas críticas, pode, até mesmo, custar a vida de diversas pessoas. Devido a isso, existe uma alta necessidade de controle minucioso do meio cibernético por parte das forças armadas, o que envolve ações ofensivas e defensivas [4].

Desta forma, fica clara a necessidade das forças armadas em buscar, cada vez mais, a eficiência no meio cibernético. A partir desse contexto, essa dissertação visa propor um conjunto de habilidades necessária aos *cyber red teams* militares e também uma metodologia de treinamento contínuo, com o objetivo de tornar as ações feitas nesse meio mais eficazes.

1.1 CONTEXTUALIZAÇÃO

A guerra cibernética segue alguns princípios que são diferentes da guerra convencional, caracterizada por acontecer em ambiente físico. A ausência de limitações físicas e a dificuldade em se identificar o ator das ações são alguns dos maiores desafios para essa vertente de guerra. Isso tudo sem levar em conta que, mesmo não acontecendo no contexto físico, a guerra cibernética pode acarretar em consequências cinéticas de grande impacto [1]. Embora a cibernética seja um campo de guerra já conhecido a bastante tempo [5], nos tempos atuais o termo ganhou mais força, tomando cada vez mais espaço nas organizações, pois seus impactos vêm trazendo grandes prejuízos aos alvos [6].

As ações feitas por órgãos militares no meio cibernético evidenciam pouco a pouco a necessidade de conhecimento avançado na área, por parte de todas as forças armadas do mundo, pois já existem diversos casos onde comprovadamente aconteceram operações militares cibernéticas [4]. Em alguns casos de ataques cibernéticos, pelo contexto político-diplomático e a analise apurada das declarações de chefes de Estados em tensão, pode-se supor a ocorrência de atividade militar, no entanto não foram assumidas oficialmente. Também existem casos que são sigilosos onde pela falta de evidências, sequer pode-se supor a autoria ou participação militar. O caso Stux-

net é um bom estudo de caso [7], demonstrando claramente a criticidade desse assunto. Neste ataque observa-se por exemplo que até mesmo os sistemas imensamente especializados (e.g., controle e automação de usinas nucleares) devem estar entre as capacidades das forças armadas, considerando-se o ambiente cibernético.

O Stuxnet foi um *worm*, desenvolvido para afetar, de uma forma eficiente e sorrateira, um sistema tipo SCADA fabricado pela Siemens e utilizado para controlar centrífugas de enriquecimento de urânio no Irã [7]. O ataque com Stuxnet nas usinas nucleares do Irã, juntamente com a falta de habilidades necessárias pela equipe local naquele momento, ocasionaram grandes perdas.

Além de conseguir realizar extravio de dados contidos na usina, esse ataque também foi capaz de danificar muitas centrífugas, pois alterava de modo imperceptível sua rotação. Esse fato, levavam-nas a danificarem com frequência e, assim, impediam o bom andamento dos projetos de enriquecimento de urânio do Irã [7].

Com o objetivo de se preparar melhor para os desafios no campo da cibernética, as organizações militares inicialmente implementaram validações mais ofensivas de seu sistemas, ação muito conhecida como *pentest* ou teste de penetração [8]. O teste de penetração se caracteriza pelo emprego metódico de diversas técnicas de invasão em sistemas computacionais e visa mapear o maior número de vulnerabilidades possíveis [9]. Essa atividade é muito requisitada no meio comercial e em alguns órgãos públicos. O teste de penetração costuma trazer resultados satisfatórios após a sua realização, o que causa diminuição das vulnerabilidades nos sistemas das organizações de um modo geral.

Algumas organizações que trabalham com dados sensíveis, como as organizações militares, também podem optar por contratar mercenários ou alguma empresa que possua uma equipe cibernética à disposição [6], para realizar o trabalho. No entanto, essas equipes defensivas e ofensivas, que serão contratadas, terão acesso às informações confidenciais que devem ser apenas de uso interno. Ao fazer essa contratação, a organização assumirá o risco de ter seus dados extraviados por terceiros, já que existem grupos que, comprovadamente, se camuflam de empresas de segurança para obter acesso aos dados dessa natureza [10].

Além de não ser recomendado que uma organização militar tenha esse tipo de postura por lidar com dados sensíveis, percebeu-se também que o teste de penetração não atenderia a todas as necessidades. Por isso, decidiu-se então, pela implementação de times cibernéticos, de forma a construir equipes especializadas em subáreas da segurança da informação, como nas partes de segurança ofensiva e defensiva separadamente. Com isso, pode-se se testar as defesas de um modo mais profundo, amplo e especializado [6].

Mais recentemente, as forças militares passaram a colocar em operação os times cibernéticos, para realizar melhor suas operações e treinamentos militares. Neste contexto, a OTAN (Organização do Tratado do Atlântico Norte), que é uma organização internacional para assuntos militares, implementou os times cibernéticos para melhor realizar e organizar suas operações militares [11]. Como a OTAN é uma organização referência e conta com a participação de diversos países ativos na área de cibernética, vários outros países, mesmo que não membros da organização, passaram

a seguir esse mesmo modelo, como exemplo de implementação [12].

Antes de serem equipes dedicadas para a cibernética, elas já eram utilizadas dentro de contexto militar a muito tempo, divididas basicamente em duas, o *red team* e o *blue team*. Essas expressões foram originadas da época da "guerra fria"[5], onde o conceito de *red team* e *blue team* passaram a ser conhecidos pelos militares como uma maneira de pensar e simular a ação do inimigo, em conjuntos com as estratégias de defesa da própria organização [11].

Os *red teams* e os *blue teams* são ainda utilizados nos exercícios operacionais de guerra pelas forças militares no mundo todo. De um modo geral, o *red team* é responsável pela parte ofensiva do exercício, e simula o inimigo, já o *blue team* representa a parte defensiva, ou seja, simula a própria organização [3]. Desse conceito surgiram as equipes *cyber red team* e *cyber blue team* na cibernética, conforme são chamadas dentro e fora dos exercícios operacionais militares [11].

Como o *cyber red team* e o *cyber blue team* passaram a ser parte integrante das forças armadas, significa que eles devem ser tratados como uma tropa de guerra e também devem estar altamente preparados para colaborar com seus respectivos países, mediante a um conflito [2]. Dessa forma, a organização poderá estar sempre um passo à frente de agentes maliciosos e, até mesmo, das forças armadas de outros países que não estão maduras nesse modelo de guerra. Isso sempre caracteriza uma vantagem, pois a qualquer momento, um país pode se tornar um rival de guerra. Esse cuidado com a cibernética é sempre em relação a proteção da sua população, território e infraestruturas. Essa ação, não visa em momento algum incentivar conflitos, apenas sim, reforçar a importância da estruturação da cibernética nas forças armadas. Isso é altamente necessário, já que até criminosos cibernéticos podem utilizar das fragilidades de um país para causar grandes danos a toda sua população.

Mediante ao exposto, fica claro que para sobrevivência de um Estado nos dias atuais diante de uma guerra, é altamente necessário que suas forças militares possuam os *cyber teams* preparados [13]. Para o sucesso na guerra cibernética, as forças militares devem ser capazes de realizar com excelência, três de seus princípios, sendo eles a defesa cibernética, a exploração cibernética e o ataque cibernético. Esses três princípios devem ser realizados em conjunto com a busca constante por informações neste meio [14], atividade conhecida como inteligência. A eficiência nas ações de inteligência em uma guerra cibernética pode determinar a predominância nesse ambiente. A atividade de inteligência também conta com informações de todos dos domínios além da cibernética, como terrestre, marítimo, aéreo e aeroespacial [15]. Esses outros domínios, fornecem informações que quando cruzadas com as obtidas no ciberespaço, podem, até mesmo, determinar o resultado final da guerra.

Com todas essas competências corretamente incorporadas a uma força militar, um Estado será capaz de realmente fazer uma projeção de seu poder militar de uma forma completa [16]. No entanto, não se deve esquecer que a integração entre todos os ambientes de batalha dentro de uma guerra será fator diferencial, pois apesar de uma guerra poder ser travada apenas no ambiente virtual, essa não é uma regra. Devido a isso, a força militar deve ser capaz de tirar proveito em todos os ambientes onde a guerra pode acontecer. Para facilitar esse entendimento, algumas doutrinas

de guerra feita por Estados, como no caso do Brasil, já trazem esse conceito e denominam cinco ambientes de guerra, sendo eles: terrestre, marítimo, aéreo, espacial e cibernético [15].

Todavia, por mais que a existência das equipes cibernéticas nas forças armadas seja um requisito para a eficiência da força militar no campo, o ciberespaço é complexo e precisa ser estudado corretamente antes de qualquer atitude. Esse espaço é altamente mutável e as tecnologias evoluem muito rapidamente, portanto, as equipes cibernéticas sempre precisam adquirir novas habilidades e treinar para manter as antigas [11]. Tudo isso é independente do nível ao qual a equipe se encontra atualmente. A falta de um conteúdo direcionado para as equipes cibernéticas das forças armadas, em relação a uma guerra cibernética, faz com que existam dificuldades no processo de identificação dessas habilidades necessárias, que nas forças armadas são altamente específicas, devido ao seu contexto de aplicação.

Como se trata de um conteúdo militar e é direcionado às estratégias e táticas de guerra, os Estados tendem a não fazer uma ampla divulgação do conteúdo sobre seu domínio. Isso deve-se ao fato que uma estratégia não deve ser divulgada, para que a vantagem cibernética dure o maior tempo possível. Com isso, tem-se a carência do conteúdo científico e isso faz com que os outros Estados criem suas equipes e treine as suas habilidades de um modo que pode não ser eficiente. A ação dos Estados com poucos recursos para desenvolver a sua metodologia, pode mantê-los em um estado vulnerável, não só ao ataque de outro país como também à ataques de criminosos cibernéticos [2].

A identificação das habilidades necessárias para as equipes cibernéticas no contexto militar não é o único desafio. A forma com que essas equipes devem ser empregadas também carecem de informação. O ambiente militar é muito reservado e não costuma divulgar os seus passos. Como essas informações pertinentes a formação eficiente dos *cyber teams* e metodologias de treinamento e emprego , em grande parte, são feitas de forma reservadas, muitos Estados podem encontrar grandes dificuldades em estruturar, iniciar e manter esses aspectos com a eficácia necessária [17].

Portanto, chega-se à conclusão de que existe uma dificuldade, natural e recorrente nas forças armadas de se adaptar ao novo cenário da cibernética, presente em guerras contemporâneas. Essa dificuldade afeta principalmente os países com menos recursos, que correm os mesmos riscos de grandes países e se tornam mais vulneráveis por não disporem dos recursos necessários. Essa vulnerabilidade, pode colocar em risco a população e todo o território, que podem sofrer grandes impactos principalmente se as infraestruturas atingidas forem críticas.

Para o fim de colaborar com as equipes militares, este trabalho apresenta uma proposta de habilidades inerentes aos *cyber red teams* no contexto militar. Para isso foram levadas em consideração várias referências relativas às equipes cibernéticas e também às operações militares. O *cyber red team*, a equipe ofensiva, realiza o seu treinamento e eleva o *cyber blue team* ao seu nível, após a simulação de um confronto. Com um mapeamento claro das habilidades necessárias aos *cyber red teams,* pode-se empregar melhores parâmetros para seleção de profissionais e torná-los ainda mais capacitados ou então, até mesmo, preparar os profissionais que sejam próximos

das habilidades para algumas atividades específicas, de modo a economizar recursos e realizar a atividade de forma eficiente.

Junto à proposta de habilidades para o *cyber red team* militar, este trabalho também propõe uma metodologia de treinamento contínuo que não exige que os profissionais, pertencentes a ambas equipes, se envolvam exclusivamente aos exercícios. Isso difere a metodologia desenvolvida neste trabalho das demais existentes que serão comparadas ao decorrer do trabalho. No entanto, o fato da metodologia não exigir dedicação exclusiva, não a limita, pois mesmo com essa característica, ela permite um aumento constante das habilidades cibernéticas, com vantagem de não levar qualquer prejuízo ao trabalho real.

A metodologia proposta foi aplicada em uma organização militar real. Isso foi possível devido à colaboração de diversos profissionais dessa organização. Com isso foi comprovado que as equipes cibernéticas poderão, em um contexto militar, aumentar e manter suas habilidades paralelamente ao emprego real. Tudo isso, foi possível sem impactar negativamente a organização e principalmente sem expor suas características e as informações sensíveis sobre sua guarda.

1.2 MOTIVAÇÃO

Este trabalho foi desenvolvido no intuito de orientar os tomadores de decisão, principalmente em estruturas com menor índice de desenvolvimento, no processo de construção de equipes de cibernética nas suas forças armadas, em especial o *cyber red team*. A partir da definição das competências dos *cyber red teams*, espera-se que o setor tático das forças armadas possam selecionar e desenvolver metodologias para recrutamento de pessoal, de uma forma eficaz. Na mesma proporção, espera-se que as forças armadas sejam capazes de prever os treinamentos necessários antes do emprego operacional do *cyber red team*. O conhecimento prévio dessas competências permite uma melhor estruturação da equipe, de forma que o setor operacional possa cumprir eficazmente todos os objetivos estratégicos e táticos exigidos para o meio militar, e também elevar o nível do *cyber blue team*, a partir de exercícios mais sofisticados.

Ao construírem equipes cibernéticas para suas forças armadas de modo eficaz, os países tornam-se, mais independentes e protegidos dos ataques cibernéticos. Esses impactos derivam, normalmente, de ataques feitos aos serviços essenciais para qualquer Estado. Como nos dias atuais, a população de qualquer país está sob total dependência de sistemas computacionais, como sistema de telecomunicações, sistemas de energia (e.g., hidroelétricas), sistemas de controle de tráfego aéreo, etc, o prejuízo a qualquer um desses serviços pode causar grandes impactos, que podem inclusive ser irreversíveis [9].

Devido à globalização e a dependência econômica entre países, um ataque cibernético bem sucedido pode colocar em risco, mais do que apenas a população do país alvo. No entanto, não basta apenas conhecer as habilidades necessárias e construir suas equipes cibernéticas militares. Para proteger a nação, essas equipes, precisam estar em evolução constante, sem afetar a produtividade

no trabalho cotidiano.

1.3 OBJETIVOS

Este trabalho tem por objetivo geral identificar e apresentar de forma clara e objetiva as competências inerentes a um *cyber red team* no contexto militar, bem como de desenvolver uma metodologia de treinamento contínuo para que o *cyber red team* e o *cyber blue team* tenham uma evolução contínua e eficaz de suas habilidades, sem prejuízo ao trabalho cotidiano.

Espera-se contribuir dessa forma, para que as forças armadas de um país estejam melhor preparadas para realizar as operações no caso de uma guerra cibernética, projetando melhor o seu poder militar, e também protegendo toda uma nação contra os mais variados tipos de ataques cibernéticos.

1.3.1 Objetivos específicos

- Identificar um conjunto de habilidades necessárias a construção de *cyber red teams* militares.
- Desenvolver uma metodologia que concilie o trabalho real cotidiano com o treinamento contínuo.
- Avaliar conceitos de aplicação prática de testes de segurança.
- Comparar resultados obtidos ao longo da aplicação prática da metodologia proposta.
- Gerar conhecimento situacional sobre as equipes cibernéticas para os tomadores de decisão do órgão militar.

1.4 PUBLICAÇÕES

O artigo "Competências para os *cyber red teams* no contexto militar"[3], referente ao assunto tratado no terceiro capítulo desta dissertação, foi apresentado na ICITS'20 (Conferência Internacional Tecnologia da Informação e Sistemas de 2020), realizada na Universidade Distrital Francisco José de Caldas, em Bogotá, Colômbia, entre os dias cinco e sete de fevereiro de 2020 [18].

A publicação do artigo foi feita na RISTI (Revista Ibérica de Sistemas e Tecnologias de Informação), na edição RISTI, N.º E26, 02/2020. A RISTI é uma revista científica pertencente a AISTI (Associação Ibérica de Sistemas e Tecnologias de Informação) e seu ISSN é 1646-9895. Essa revista tem o seu foco na investigação e na aplicação prática e inovadora dos sistemas e das tecnologias de informação de forma geral. É um periódico trimestral que publica artigos originais

e inovadores, em português e espanhol. o artigo é aceito num processo de avaliação que passa por, pelo menos, três membros do Conselho Científico [19].

1.5 ORGANIZAÇÃO

Esta dissertação está organizada da seguinte forma:

- No Capítulo 1 é feita uma introdução ao tema da dissertação, exibindo os aspectos necessários para o entendimento do trabalho. Apresenta também a motivação e os objetivos do trabalho, além de relatar os resultados preliminares em termos de publicações .
- O Capítulo 2 referencia os trabalhos que foram utilizados como base para o estudo, entre eles, diversos estudos sobre *cyber red team* e *cyber blue team*, e sobre os conceitos de guerra cibernética.
- No Capítulo 3 são apresentadas e discutidas detalhadamente as competências que um *cyber red team* deve possuir no contexto militar.
- O Capítulo 4 apresenta a metodologia de treinamento proposta. Mostra todas as suas premissas e exibe também os resultados preliminares obtidos com a sua aplicação, dentro de um laboratório.
- No Capítulo 5 são apresentadas as conclusões do trabalho com destaque para as vantagens e desvantagens observadas durante a aplicação prática da metodologia. Termina com algumas sugestões para trabalhos futuros.

2 FUNDAMENTAÇÃO

Para atender os requisitos necessários para a projeção do poder militar na guerra cibernética, foram analisados diversos estudos. Entre os fatores analisados estão os estudos das áreas as quais dependem uma guerra cibernética e os principais termos utilizados. Foram exibidas nesse capítulo as ações pré-existentes que são atualmente empregadas em conjunto das habilidades propostas por diversos autores da área. Esse capítulo exibe os estudos que foram adaptados e aperfeiçoados para o contexto e assim contribuem para o cumprimento do objetivo desta dissertação.

2.1 CIBERESPAÇO

O ciberespaço pode ser definido como um domínio global, um ambiente de informações que consiste em diversas redes de comunicação interdependentes, como a Internet. No entanto, não se resume apenas à Internet e sim a todas as redes de telecomunicações, sistemas de computadores, processadores e controladores. O ciberespaço compreende todo ambiente que conecta dispositivos que possam trocar informações [14].

Em meio ao ciberespaço acontecem as ciber operações, também conhecida como *CyberOps*, operação que, geralmente, é feita por órgãos militares ou de inteligência. Esse tipo de operação se resume ao emprego de recursos cibernéticos, onde o objetivo principal é alcançar objetivos estratégicos ou tático impostos, por meio do ciberespaço [14].

2.2 *CYBERANGE*

Um *Cyberange* é uma parte integrante do ciberespaço, correspondendo a uma infraestrutura importante para avaliar novas tecnologias de cibersegurança. A partir dele pode-se efetivamente suportar novas verificações de segurança de rede, testes de ferramentas de intrusão ofensivas e defensivas, exercícios onde há confronto e a avaliação de riscos das redes[20].

A principal função de um *Cyberange* é fornecer um ambiente, que represente o mais próximo possível a realidade, para a realização de testes de segurança de rede e fornecer avaliações quantitativas e qualitativas de várias tecnologias de rede [21]. Um *cyberange* pode ser visto como uma rede controlada, normalmente separada das demais e implementando uma função específica. As ações que normalmente ocorrem em um *cyberange* podem gerar riscos se conectadas às redes funcionais.

O ambiente cibernético, em um contexto militar, permeia todos domínios de guerra [15]. Grandes impactos cinéticos podem ocorrer em virtude de ações no meio cibernético, ainda mais

quando leva-se em conta as infraestruturas críticas que, se afetadas, trazem enormes prejuízos a todo um país. Como a implantação de *cyber red teams* tem sido recorrente em diversos países e organizações como a OTAN, a utilização desses *cyberanges* para realizar exercícios também se torna uma realidade para manter as equipes cibernéticas preparadas para ações no contexto militar [11].

A preocupação com o ambiente cibernético torna-se cada vez mais intensa no meio militar, pois, a partir dos princípios da guerra cibernética é possível realizar ações com grandes efeitos cinéticos danosos. Esses danos podem ser altamente prejudiciais como, por exemplo, a abertura indesejada das comportas de uma barragem ou o desligamento de uma subestação elétrica, entre outros. [1]. Por meio de *cyberanges* é possível criar ambientes segregados para simular ataques nessas circunstâncias.

2.3 GUERRA CIBERNÉTICA

Uma guerra pode acontecer de várias formas e fazendo uso de diferentes meios, como o terrestre, marítimo, aéreo, espacial e cibernético [15]. Foi exatamente desse conceito que surgiu a palavra *warfare* nos Estados Unidos, significando o meio em que se desenrolará uma guerra, podendo ser um ou vários ao mesmo tempo [22].

O termo *warfare* ficou muito popular ao se juntar com a palavra *cyber*, redução de *cybernetics*. Com isso, o termo *Cyber warfare* passou a ser utilizado como um termo global que em português chamamos de guerra cibernética. A guerra cibernética é um movimento atual, refletindo os meios de comunicação existentes nos dias de hoje [23].

Uma guerra cibernética não possui as mesmas características de uma guerra convencional que acontece em ambientes cinéticos. Em uma guerra cibernética existem algumas peculiaridades e conceitos como a ausência de limitações físicas, possíveis efeitos cinéticos, discrição, mutabilidade, inconsistência, falta de identidade e privilégios, dualidade, controle de infraestrutura e informações conforme o ambiente operacional [1]. Ao levar em consideração esses princípios e conceitos, as forças militares devem ser capazes de realizar atividades de defesa cibernética, exploração cibernética e ataque cibernético [14].

Em [1], foi feito um estudo diretamente ligado à identificação das características da guerra cibernética, diferenciando-as de uma guerra cinética convencional.

Tabela 2.1: Peculiaridades de uma Guerra Cibernética

Principio	Descrição
Ausência de limitações físicas	Limitações físicas de distância e espaço não se aplicam no mundo cibernético. No ciberespaço, a distância física não é um obstáculo nem um facilitador para a realização de ataques. Um ataque cibernético pode ser executado com igual eficácia do outro lado da Terra e de uma sala ao lado.
Consequências cinéticas	A guerra cibernética pode afetar diretamente objetos no mundo físico, como a abertura de um portão de uma barragem, desligamento de uma subestação elétrica, etc.
Anonimidade	No ciberespaço é possível tomar medidas ativas para se esconder, mas tudo o que se faz é visível. Esconder-se no mundo cibernético é análogo ao uso de camuflagem no mundo físico. Os combatentes cibernéticos podem modificar ou disfarçar seus rastro, por meio do uso de tecnologias furtivas.
Mutabilidade & Inconsistência	O ciberespaço é mutável; portanto, a guerra cibernética não é consistente nem confiável. Esse princípio era originalmente dois princípios separados, mas como eles são inter-relacionados, foram combinados.
Identidade & Privilégios	Existem entidades que têm certo nível de autoridade e acesso ou a capacidade para executar alguma ação que seja restrita. Essa identidade pode ser assumida por outra entidade, ao aproveitar uma vulnerabilidade ou simplesmente ao uso de técnicas de engenharia social.

Principio	Descrição
Dualidade	As atividades de defesa ou de ataque na guerra cibernética podem usar as mesmas ferramentas. Isso envolve o uso de *Scanners* de vulnerabilidade, que por exemplo, são usados em ataques e em defesas, para descobrir as vulnerabilidades. A diferença entre eles se dá no modo de uso, pois um irá explorar e o outro corrigir as vulnerabilidades. Outro fato importante, é que uma falha descoberta em um sistema comum, se transforma em uma arma e também uma vulnerabilidade ao mesmo tempo.
Controle de infraestrutura	Apenas uma pequena parte do ciberespaço é controlada e utilizada realmente. Quem controla umas das partes do ciberespaço que o oponente usa pode controlar o oponente, ou impor pelo menos, algumas restrições.
Informação como ambiente operacional de guerra	Tudo o que envolve a guerra cibernética é informação. As comunicações, mapas de rede, listas de funcionários, sites, links, e-mails, postagens e todos os outros aspectos do alvo já são informações no ciberespaço.

Conforme a Tabela 2.1 evidencia, a guerra cibernética é diferente da guerra cinética convencional. Uma das diferenças fundamentais entre a guerra cibernética e a guerra cinética é a natureza de seus ambientes. A guerra cinética ocorre no mundo físico, governado por leis físicas. A guerra cibernética ocorre em um mundo artificial, que muda constantemente [1].

2.4 PROJEÇÃO DO PODER MILITAR NA GUERRA CIBERNÉTICA

Um Estado pode projetar sua força sobre outro de várias formas, entre elas a diplomática, a comercial e a militar. Uma projeção de poder significa que, por meio do uso da força, um ator é capaz de dobrar a vontade de outrem. A intervenção militar é uma forma de projeção de poder que, geralmente, está presente em guerras declaradas. Nessas guerras, o poder político ou o alto comando das forças armadas de um Estado estabelecem metas as serem cumpridas, juntamente com a magnitude e a duração das operações militares de combate [16].

Para uma projeção de poder militar em uma guerra cibernética, é necessário que as forças armadas tenham sob seu comando, os profissionais mais preparados nos três maiores princípios que a regem: defesa cibernética, reconhecimento e ataque cibernético [14]. A defesa cibernética

deve ser feita não apenas pelas forças militares, mas por todas as organizações. O reconhecimento e o ataque já são inerentes as forças armadas, no entanto, agentes criminosos também pode fazer uso destes conceitos.

A projeção do poder militar na guerra cibernética dependerá do quão eficientemente as forças armadas são capazes de realizar as três ações que são pré-requisitos. À princípio, o reconhecimento cibernético faz uma grande diferença, pois a partir dele é possível conhecer o seu inimigo e, por isso, proporciona grandes vantagens. Com isso, chega-se à conclusão que a inteligência cibernética é um fator fundamental para determinar a superioridade do país no ciberespaço [24]. A inteligência cibernética é uma habilidade que deve estar em constante utilização, para que em um momento crucial, as informações por ela gerada sejam de valor as forças armadas e ajudem a proporcionar a projeção do poder.

2.5 *CYBER TEAMS*

As expressões *red team* e *blue team* tiveram origem na "Guerra Fria", pois sempre esperavam um ataque do inimigo e a simulação com essas equipes era vista como uma forma de se preparar para isso. Essas equipes são, até hoje, utilizadas dentro das forças armadas e costumam ser empregas em qualquer tipo de exercício operacional [11] [3]. O mesmo conceito é utilizado em desafios na Internet, conhecidos como CTF (*Capture The Flag*), onde o *red team* tem que capturar uma *flag* com emprego ofensivo e o *blue team* tem que evitar que isso ocorra [25] .

Utilizar as equipes cibernéticas (*cyber teams*) nas forças armadas, nada mais é do que uma forma de segregar um trabalho em subáreas e avançar e em relação à especialização. As equipes são compostas por pessoas que estarão preparadas para trabalhar de forma ofensiva, defensiva ou em alguma atividade específica que justifique uma segregação, a fim de atingir os objetivos estratégicos e táticos da sua organização [3].

No contexto militar, existem vários *cyber teams* possíveis e cada um tem suas responsabilidades e habilidades [13]. A projeção de poder militar na guerra cibernética depende da eficiência dos times nas suas devidas subáreas. Para realizar operações cibernéticas, a organização militar deve ter equipes cibernéticas que atinja o maior nível possível em suas habilidades [11] e a construção desses *cyber teams* especializados, ajuda neste objetivo [3].

Na metodologia que será apresentada nesta dissertação, trabalhar-se-á com três *cyber teams*. O *cyber red team* e o *cyber blue team*, para a parte ofensiva e defensiva respectivamente, e o *cyber purple team*, que pode ter diferentes modos de ação. A ação do *cyber purple team* depende da referência utilizada, e no contexto deste trabalho será uma equipe de gerência responsável pela comunicação entre as equipes. Nas seções abaixo é detalhado significado de cada equipe para o contexto deste trabalho.

2.5.1 *Cyber blue teams*

O *cyber blue team* é responsável por toda a defesa da organização. Essa equipe representa nos exercícios a própria organização que pertence e portanto, eles também devem ter uma ampla gama de habilidades. As habilidades que essa equipe cibernética deve possuir incluem implantação de ativos de defesa, monitoramento constante, análise forense digital, tratamento de incidentes na rede e até fatores como inteligência de ameaças devem ter uma forte maturidade profissional [26] [3].

O *cyber blue team* deve estar atento aos profissionais que ingressam na equipe ou na organização, pois eles podem significar riscos à segurança. Naturalmente, mesmo não chamados como *cyber blue team*, toda organização possui o seu, pois de alguma forma, alguém é responsável pela segurança. Então, o *cyber blue team* é uma equipe que é sempre existente e tem prioridade na montagem, já que proteger é prioridade [11] [3].

2.5.2 *Cyber red teams*

A utilização dos *cyber red teams* no contexto da cibernética está sempre ligada ao oponente. O *cyber red team* representa o risco para o *cyber blue team*. No entanto, com a expansão da cibernética e sua grande utilização como ambiente operacional de guerra [15], viu-se a necessidade de manter o *cyber red team* de modo permanente nas forças armadas, como uma tropa especializada. No contexto militar, o *cyber red team* tem o objetivo de constituir uma frente operacional de guerra no ambiente cibernético [1] e não mais apenas de realizar simulações de ataques em exercícios de guerra [3].

Os *cyber red teams* não se restringem apenas ao meio militar, sendo também fornecidos por empresas de segurança, como um serviço, para avaliar de modo completo as defesas de seus clientes. Dessa forma, um *cyber red team* pode ser percebido equivocadamente como uma metodologia de teste de penetração [10]. No entanto, é importante ressaltar que estas são atividades distintas, já que o *cyber red team* atende a um escopo muito mais amplo, profundo e especializado do que o teste de penetração ou *pentest*, como também é conhecido [6] [3].

2.5.3 *Cyber purple teams*

O *cyber purple team* é uma equipe que surgiu a partir de estudos mais recentes, devido à necessidade de se ter um ponto de interlocução e controle, especializados, nos exercícios de cibernética [27]. Os *cyber purple teams* são responsáveis pela comunicação entre todas as equipes de um exercício, mas também podem ser aplicados fora de um, sendo capaz de gerar estatísticas sobre os times, transmitir isso ao alto comando e colaborar, assim, para o direcionamento das ações.

Os *cyber purple teams* podem compartilhar informações, mudar o foco de um exercício e também podem indicar modos de ação [27]. Essa equipe possui o roxo como cor, por ser a com-

binação do vermelho e o azul, o que indica uma mistura, algo central. No entanto, a nomenclatura não é padrão e dependendo da referência utilizada pode ser tratado das mais variadas cores e com as mais variadas funções. Independentemente do nome que assuma ou a sua cor nas outras referências, para este trabalho, ela é a equipe que gerencia todos os exercícios e suas infraestruturas. Dessa forma, também é a equipe responsável pela comunicação, pela coleta dados e pela geração de informações, com o objetivo de identificar pontos a serem trabalhados nas equipes.

2.6 GESTÃO DOS *CYBER TEAMS* SOB UMA GUERRA CIBERNÉTICA

Observa-se que existem cargos de gerência fixa no contexto dos *cyber teams* e também em níveis hierárquicos superiores, aos quais todas as equipes são subordinadas. No caso, o chefe do *cyber red team* é representado como *head* e outras áreas também possuem a sua chefia. Os cargos de chefia são de alta importância para todas as equipes, pois deles, derivam os objetivos e é eles também que promovem os meios.

Para a administração das equipes, os seus respectivos líderes devem obedecer ao conceito geral de administração de equipes sendo capaz de realizar todas as atividades burocráticas e de recursos humanos. Em [28], define-se as habilidades necessárias a um administrador, que por sua vez, deve ser capaz de planejar, organizar, dirigir e controlar todos os processos inerentes as equipes, obedecendo a hierarquia organizacional. Na Figura 2.1 exibe-se a conjunção de habilidades e conhecimentos que devem ser somados para a formação de um profissional de sucesso da área administrativa [28].

Uma outra função fixa que também é característica dentro do *cyber red team*, e no caso se restringe apenas a essa equipe, mostra a necessidade de se ter um líder técnico para cada subtime de ataque estabelecido. Então para cada objetivo imposto pela alta gestão serão definidas sub-equipes especialistas com um líder técnico em cada uma.

Os líderes técnicos se concentram em três funções principais: compreender o problema, gerenciar o fluxo de ideias e a manutenção da qualidade. Essas funções são os ingredientes que caracterizam o que chamamos de estilo de liderança na solução de problemas. Esse é o estilo que caracteriza os melhores líderes técnicos [29].

2.7 *CYBER RED TEAM* VERSUS *PENTEST*

A possibilidade de grandes prejuízos causados por meio do domínio cibernético obriga as forças armadas a implementarem projetos de defesa complexos, mas sempre há dúvidas acerca da eficiência, mediante a ataques reais. Para tentar validar seus sistemas quanto à segurança, as organizações geralmente utilizam o *pentest*, no entanto, apenas isso não é capaz de avaliar todas as suas defesas. Por exemplo, o *pentest* não é capaz de avaliar deficiências humanas, tecnológicas

e de processos em conjunto. Por outro lado, como os *cyber red teams* costumam ser fornecidos por empresas como um serviço [6] acabam por ser confundidos com uma metodologia de *pentest*, até mesmo pela própria organização prestadora do serviço.

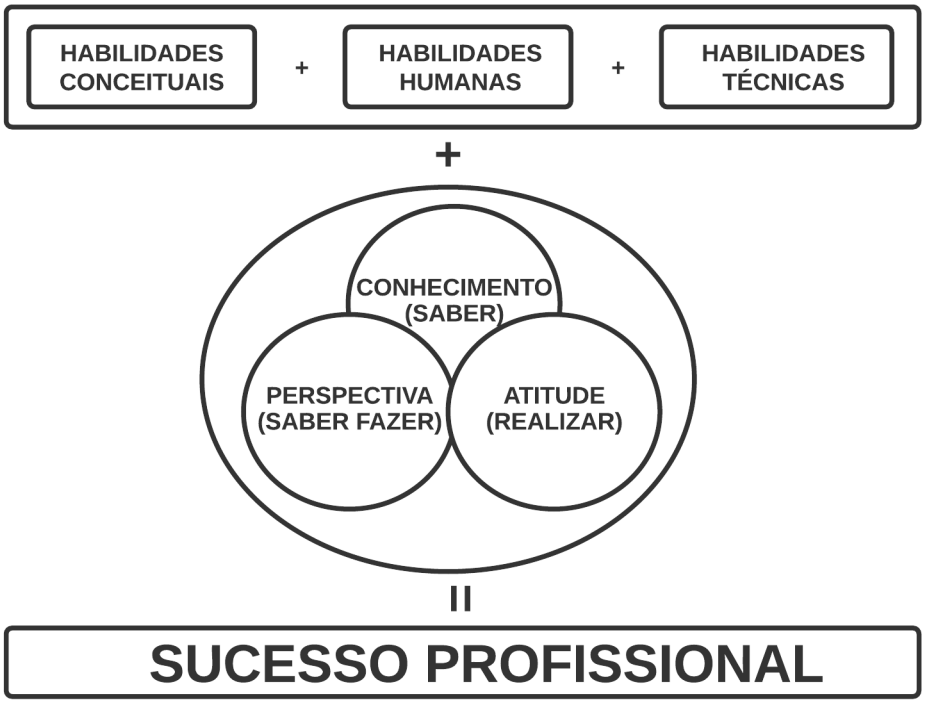

Figura 2.1: Habilidades recomendadas para os administradores

O *pentest* visa encontrar o maior número de vulnerabilidades em um sistema e para isso segue à risca alguma metodologia para simular ataques, de forma a avaliar o quão vulnerável é um sistema [30]. Já o *cyber red team* é guiado por objetivos e seu alvo é sempre uma organização. O *cyber red team* deve ser composto de especialistas que sejam capazes de compreender os interesses, intenções e capacidades do alvo, a fim alcançar os objetivos [5]. A missão do *cyber red team* é emular as táticas, técnicas e procedimentos (TTPs) dos oponentes, com objetivo de fornecer os fatos concretos, para que a postura de segurança de uma organização seja aumentada [30]. No contexto militar, leva-se em conta também, sua utilização para manter a superioridade mediante uma guerra cibernética [24]. A Tabela 2.2 resume as principais características diferenciando o *pentest* do *cyber red team*.

Tabela 2.2: Principais características que diferenciam o *pentest* do *cyber red team*

	Pentest	***Cyber red teams***
Metodologias	Utiliza de forma sistemática metodologias como: *PTES* [8], *OSSTMM* [31], *ISSAF* [32], *OWASP* [33], entre outras.	Flexível. Não são obrigatórias, porém podem ser utilizadas por completo, em parte ou serem adaptadas, conforme as necessidades para o cumprimento dos objetivos.

Tabela 2.2: Principais características que diferenciam o *pentest* do *cyber red team*

	Pentest	***Cyber red teams***
Escopo	Restritivo, geralmente anunciado, sistema ou infraestrutura alvo.	Toda a organização, geralmente não anunciado, testar *blue teams*, políticas, ferramentas e habilidades.
Técnicas	Caixa preta, cinza ou branca.	Simulação, sondagens de vulnerabilidade, análises alternativas.
Objetivo	Encontrar vulnerabilidades.	Realizar explorações, em prol de um objetivo previamente definido.
Emprego	Em razão da defesa cibernética.	Em equipes de segurança cibernética, inteligência e no contexto militar.

2.8 TRABALHOS CORRELATOS

Diversas obras já trabalharam de alguma forma o tema *red team*. No entanto, essas obras não têm o seu estudo direcionado para identificação das habilidades necessárias a um *cyber red team* no meio militar e nem criam uma metodologia para o seu emprego nesse meio. A maioria dos estudos possui maior ênfase nas técnicas de emprego de *cyber red team* de uma forma genérica. Poucas obras trabalham de forma específica a identificação das habilidades do *cyber red team* no contexto militar. Isso gera uma lacuna de conhecimento e faz com que o emprego de técnicas e metodologias não aconteçam de forma a aproveitar a maior eficiência possível. A Tabela 2.3 exibe propostas de algumas obras em relação às habilidades necessárias aos *cyber red teams* [3].

Tabela 2.3: Propostas de habilidades para *cyber red teams*

Obra	**Proposta de habilidades**
Dandurand, L. (2011, June) - Rationale and blueprint for a cyber red team within nato.	Segurança cibernética, sistemas e redes, protocolos, redes sem fio, comunicações militares, criatividade, *buffer overflow*, arquitetura de computadores, vulnerabilidades, suporte, segurança física e gestão de pessoal.
Sharma. (2018) - Hands-on red team tactics.	Engenharia social, segurança física e pentest.
Dalziel, H. (2015) - Next generation red teaming.	Eletrônica, social, física e outras.

Tabela 2.3: Propostas de habilidades para *cyber red teams*

Obra	Proposta de habilidades
Brangetto, P., Caliskan, E., & Roigas, H. (2015) - Cyber red teaming-organisational, technical and legal implications in a military context.	Vulnerabilidades nos sistemas ou em operador humano.
Eom, J., Kim, N., Kim, S., & Chung, T. (2012, June) - Cyber military strategy for cyberspace superiority in cyber warfare.	Estratégias, táticas, infraestrutura e cibernética, outros meios que afetem a cibernética.

A estrutura de um *cyber red team* com objetivos militares já é implementada pela OTAN. Em [2], foi definido um modelo de estrutura organizacional de um *cyber red team* no contexto militar da OTAN, um modelo flexível composto na parte administrativa pelo chefe e um subchefe para o *cyber red team*, uma secretaria e um chefe específico para o suporte. A parte técnica do *cyber red team* é composta por um líder técnico para cada objetivo de ataque, acompanhado pelos demais especialistas, já a do suporte é composta por administradores de sistemas operacionais e desenvolvedores de infraestrutura e *exploits*, que são *softwares* focados na exploração de uma vulnerabilidade. Na Figura 2.2, é exibido esse modelo, de forma hierárquica [2].

Em [9], considera-se que um *cyber red team* utiliza de meios como engenharia social, segurança física e *pentest* para alcançar seus objetivos. Porém, dentro das forças armadas, algumas atividades fogem desse escopo, como por exemplo, as questões de inteligência e operações reais em espaço físico [3].

Em [34], define-se quatro competências bases para um *cyber red team*, sendo elas, eletrônica, social, física e outras. Apesar de conter bons parâmetros para definir competências, o escopo ficou extremamente grande, dificultando seu enquadramento dentro do contexto das forças armadas [3].

Em [11], considera-se que um *cyber red team*, no contexto militar, precisa encontrar e explorar vulnerabilidades nos sistemas ou em operador humano, e que para isso precisa de habilidades específicas que vão além dos conhecimentos de cibernética. No entanto, não explica com detalhes quais seriam essas competências para todo o contexto, pois, possui seu foco nas atividades de inteligência [3].

Em [24], considera-se que a superioridade em uma guerra cibernética, depende de quão bem o *cyber red team* atende às competências necessárias neste meio, exigindo, estratégias, táticas, infraestrutura e componentes que dominem de modo completo as atividades cibernéticas ou que possam ser usadas para afetá-la [3].

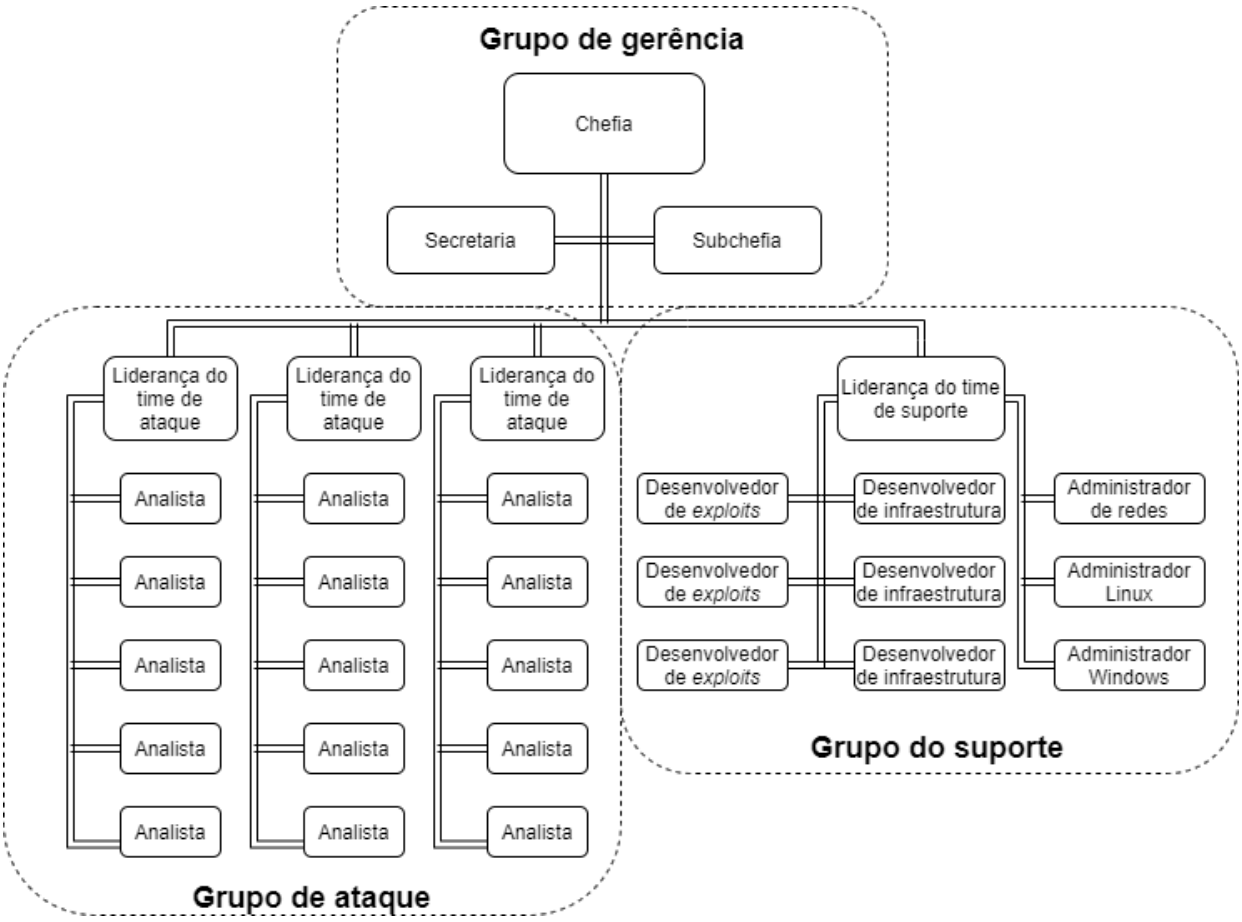

Figura 2.2: Proposta para estruturação de um *cyber red team* militar

Em [35], observa-se que a importância dos *cyber red teams* não está ligada apenas à razão de se ter uma frente operacional para guerra cibernética, mas também por ser uma maneira de aumentar a eficiência das defesas de uma forma completa, ampla e contínua, por meio do emprego da segurança ofensiva. A segurança ofensiva visa identificar e aproveitar as vulnerabilidades antes do agente mal intencionado. Isso pode ser feito por meio de *hackers* éticos, que simulam ataques contra a organização. Esse conceito claramente pode ser atendido a partir de uma estruturação correta de um *cyber red team* [17] [3].

A interação entre o *cyber red team* e o *cyber blue team* é benéfica para organização como um todo. O *cyber blue team* com o objetivo de defender a organização, consegue além de ampliar suas próprias habilidades, causar a necessidade de aumento das habilidades do *cyber red team*. Em um exercício, existe o avanço por partes, quando um time evoluiu em suas habilidades força inerentemente que o outro se aperfeiçoe para rompê-las [3] [36].

Dos trabalhos relacionados e estudados, observa-se que não há uma convergência clara e objetiva sobre a estrutura e competências que um *cyber red team* precisa para atuação no contexto militar. Nesse contexto, este trabalho pretende contribuir com uma visão mais clara das competências necessárias para um *cyber red team* militar, de forma a aumentar a eficiência de sua montagem e ação e logo após isso, propondo também uma metodologia que pretende aumentar

ainda mais as habilidades, por meio de um treinamento contínuo [3].

3 COMPETÊNCIAS DO *CYBER RED TEAM* NO CONTEXTO MILITAR

De acordo com o estudo realizado, entende-se que um *cyber red team*, no contexto militar, depende de determinadas características para sua melhor eficiência e também sua formação em si. Essas características identificadas como competências serão detalhadas a seguir.

3.1 AS COMPETÊNCIAS MACRO

De uma forma macro, pode-se identificar que no contexto militar, um *cyber red team* deve possuir quatro competências: a engenharia social para o conhecimento humano; a segurança física para ativos cinéticos; as ações cibernéticas no contexto das comunicações; e o suporte que representa as atividades de apoio, como administração, informática e conhecimentos altamente especializados em áreas não comuns [3].

A Figura 3.1, de uma forma bem ampla, apresenta em alto nível, as competências que são indispensáveis no ramo militar, neste caso inclusive, indispensável a qualquer *cyber red team*.

3.1.1 Ações cibernéticas

Dentro do conhecimento macro, denominado como ações cibernéticas, encontram-se atividades como o reconhecimento, o ataque e a manutenção de acessos no meio cibernético. Em um mundo onde até pequenos dispositivos estão conectados em rede, como celulares, relógios e outros itens que compõe a Internet das Coisas (IoT) [37], essas ações exigem, de quem irá realizá-las, grandes conhecimentos nas tecnologias de informação e comunicação (TICs). Isso inclui as ações com softwares, redes cabeadas e sem fio, tecnologias móveis, entre outras [34]. As ações de reconhecimento são necessárias pela parte de inteligência e, também, exigem conhecimentos especializados. Para um *cyber red team*, a competência cibernética é o principal fator para superioridade das forças armadas face à guerra cibernética [24] [3].

Em dias atuais, qualquer das forças armadas que não seja capaz de impor seu poder no meio cibernético, está fadada ao fracasso. Guerras cinéticas exigem um grande emprego de recursos, além de exibir uma comoção a nível mundial. Como expresso na Tabela 2.1, a guerra cibernética é totalmente dependente das ações cibernéticas, e sem isso, ela não ocorre [3].

Por exemplo, uma *botnet* é um conjunto de dispositivos infectados que são controlados por um sistema de comando e controle. Foi isso que fez a *botnet* Mirai, que era composta principalmente por dispositivos embarcados e de dispositivos *IoT* e realizou um ataque em massa na Internet em setembro de 2016. Esse ataque em massa, realizado por diversos ativos infectados ao mesmo

tempo, sobrecarregou vários alvos de altíssimo valor para diversas organizações com ataques maciços de DDoS (Negação de serviço de forma distribuída) [38].

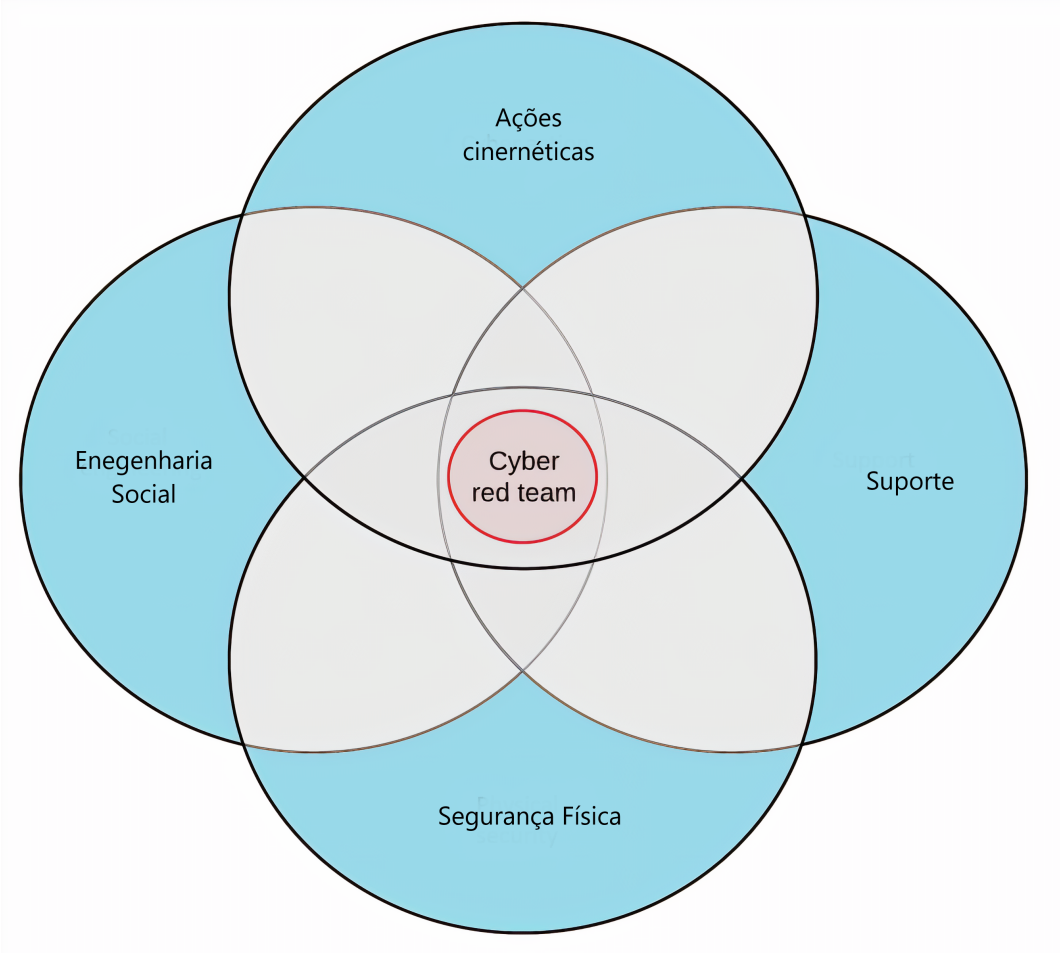

Figura 3.1: Competências macro de um cyber red team militar.

O ataque realizado pela *botnet* Mirai à empresa Krebs excedeu seiscentos Gbps, em volume, e está entre os maiores já registrados [39]. Notavelmente, esse tráfego de enorme volume foi originado de centenas de milhares de dispositivos de baixo poder computacional, componentes da *IoT* [38].

No entanto, é importante destacar que a *botnet* Mirai não foi a precursora desse tipo de ataque e metodologia. Outras *botnets* de *IoT* precederam a Mirai, como *BASHLITE* [40] e a Carna [41], esta última sendo a primeira a surgir como uma ameaça *DDoS* de alto nível [38].

Diversas outras *botnets* de grande poder podem existir. Ao analisar esse fato, nota-se com muita clareza a grande necessidade de uma força militar dominar essas técnicas. Essas técnicas serão fundamentais para a projeção de poder militar. A capacidade de se realizar negação de serviço, causará prejuízo a qualquer um dos adversários, pois a disponibilidade é um dos princípios da segurança da informação [42].

O exemplo citado, mostra a importância da competência macro de ações cibernéticas. Dentro

dessa competência macro existem diversas outras possibilidades que vão muito além do exemplo citado, abrangendo por exemplo toda a parte de telecomunicações e infraestruturas críticas, alvos frágeis para qualquer Estado e, determinantes, caso afetados em uma guerra.

3.1.2 Engenharia social

Existe uma tendência muito forte de qualquer pessoa em confiar nos fatores humanos próprios e dos outros, porém é preciso estar ciente que existem diversas formas de explorar as características emocionais de uma pessoa. A partir dessa exploração, permite-se por exemplo a extração de informações valiosas que podem ser usadas para os mais diversos tipos de objetivos e inclusive para um ataque cibernético [30]. Todos esses aspectos podem ser explorados por meio do emprego de técnicas dentro da engenharia social [3].

Um *cyber red team*, portanto, deve ser capaz de explorar o fator humano das mais variadas formas. A interação humano-computador se faz presente a todo momento e proporciona um caminho mais curto para diversos ataques. A engenharia social é uma competência importante, por propiciar grandes atalhos para o cumprimento dos objetivos [3].

Em diversos casos, o uso da engenharia social pode, até mesmo, dispensar muitos das vezes as habilidades técnicas mais complexas, exigidas na cibernética. No entanto, quando se integram a engenharia social com a cibernética, elas juntas propiciam grandes vantagens em uma guerra cibernética. Essas vantagens, geralmente, se dão por meio de ataques de *phishing* [43], via telefone, ou até mesmo, ao catalogar informações em redes sociais, tendo ou não interação direta com a vítima ou membros próximos. [34] [3].

Por exemplo, uma personalidade conhecida no ramo da cibersegurança e engenharia social é o Kevin Mitnick, que é um dos *hackers* mais conhecidos pelo emprego da engenharia social [44]. Ele utilizava técnicas de engenharia social como a *Dumpster diving*, uma técnica de vasculhar o lixo que quando era jovem, o permitiu contornar o sistema de cartões usados no sistema de ônibus de Los Angeles, nos EUA [43]. Depois que ele convenceu um motorista de ônibus a dizer onde ele poderia comprar seu próprio bilhete para um "projeto da escola", foi capaz de andar de ônibus na área da grande Los Angeles gratuitamente. Para isso ele utilizava os recibos de transferência de crédito ainda válidos que encontrava nas lixeiras ao lado da sede da empresa de ônibus [44].

Além disso, Kevin Mitnick também obteve acesso não autorizado a uma rede de computadores de uma grande empresa de telefonia nos Estados Unidos. Cerca de dez anos depois, ele foi capturado e condenado a 12 meses de prisão, seguido por três anos de liberdade supervisionada. Ainda dentro desse período, Mitnick acessou os computadores de correio de voz da empresa *Pacific Bell*, de modo não autorizado [44].

De acordo com o Departamento de Justiça dos EUA, Mitnick obteve acesso não autorizado a dezenas de redes de computadores. Chegou a conseguir uma cópia de um valioso software proprietário, usado por algumas das maiores empresas de telefonia celular dos Estados Unidos. Isso possibilitou a interceptação de diversos usuários e senhas [44].

Esse exemplo, antigo, de um ataque ainda muito utilizado nos dias de hoje, mostra a importância do conhecimento em engenharia social. Sabe-se que a espionagem internacional é uma realidade e está presente não apenas no mundo físico, mas também na exploração da interação humano-computador [45].

Uma força armada, deve ser capaz de empregar as técnicas de engenharia social. Sua utilização em todos os ambientes de guerra, traz para quem as usa grandes vantagens. A combinação das técnicas de engenharia social com a cibernética é muito atual e plausível, o que proporciona fator fundamental para a supremacia nessa vertente de guerra.

3.1.3 Segurança física

A segurança física engloba a proteção a todos os ataques que possam ser feitos e que afetem uma estrutura base para manter as tecnologias de informação e comunicação. Para além do domínio cibernético, a segurança física também pode ser melhorada por meio de técnicas empregadas pelos *cyber red teams*[5]. Deve-se levar em consideração que a segurança física é composta por vários ativos como cartões de controle de acesso, câmeras, proteções físicas para transmissão de dados, fechaduras, etc [3].

Para todos os ativos que proporcionam segurança física das estruturas existem formas de exploração [30]. Com isso, sempre existirá a possibilidade do deslocamento físico de integrantes do *cyber red team*, o que dependerá da disponibilidade de uma gama de profissionais especializados conforme o objetivo [3].

Dentro das forças armadas, a segurança física sempre foi um objetivo. Mesmo sendo essa necessidade conhecida e treinada desde os tempos mais remotos, nos dias atuais, caso seja esquecida ou mal feita pode acarretar em vantagens para o inimigo em um conflito. Uma falha que comprometa a segurança física de uma estrutura influencia fortemente nos fatores inerentes às tecnologias de informação e comunicação e à cibernética [46] [3].

Por exemplo, em [47], é feito um experimento utilizando um SBC (*Single-Board Computer*) que é uma placa avulsa que possui as mesmas funções de um computador. O uso desses dispositivos é altamente popular em vários domínios, inclusive no meio militar.

Por meio do uso de um equipamento chamado *raspberry pay*, um SBC, foi possível armazenar os dados que trafegaram na rede no dispositivo e, posteriormente, o dispositivo foi retirado e analisado, para que se fosse possível recuperar as informações trafegadas [47].

Além disso, neste experimento foi possível também realizar outros tipos de ataque de forma passiva, como o conhecido *spoofing*, onde um equipamento consegue se passar por outro [47]. Ataque muito utilizado para que os dispositivos enviem dados a um outro dispositivo não autorizado, que normalmente, se passa por um roteador.

Para realizar todas essas ações, o ator deve conseguir burlar os sistemas de segurança física como cartões de controle de acesso, câmeras, fechaduras e ainda precisa realizar uma intercep-

tação física no cabo de rede ou na entrada de rede de alguma estação de trabalho. A falta de conhecimento de vetores de ataques físicos, fizeram com que os riscos fossem ignorados ou esquecidos.

No meio militar a possibilidade de obter informações do inimigo mediante o emprego dessas técnicas, também pode definir o futuro em uma guerra, pois a informação é um valor nessa modalidade de guerra [1]. Para esse tipo de ação ofensiva nas forças armadas, pode-se até mesmo, aproveitar as ações cinéticas, para obter vantagens cibernéticas.

3.1.4 Suporte

A área de suporte é responsável pelo desenvolvimento de ferramentas, pela manutenção dos sistemas, administração das redes e criação das infraestruturas lógicas demandadas pelos times de ataque [2]. A equipe de suporte deve estar preparada para atender as demandas rapidamente, pois tanto as exigências em um ataque, quanto na defesa não podem sofrer atraso, já que esse atraso pode determinar a perda de informações sensíveis. [3].

As atividades desenvolvidas pela equipe de suporte vão além das atividades de informática. Toda atividade de apoio é inerente a essa equipe. A gestão faz parte dessa equipe e é altamente necessária ao funcionamento do *cyber red team*, pois qualquer trâmite burocrático, demandas e, até mesmo, a busca por recursos humanos necessários não podem sofrer atraso [3].

Existem também diversos conhecimentos específicos que, via de regra, não são utilizados por um *cyber red team*, mas que em situações peculiares são indispensáveis. A equipe de suporte deve ser capaz de suprir todas essas demandas, isso pode incluir conhecimentos e áreas de super especialização como aviação, enriquecimento de urânio, sistemas complexos de distribuição de energia, entre outros. Todas essas informações são trabalhadas dentro do campo de suporte, a mais heterogênea das competências necessárias ao *cyber red team* [3].

Por exemplo, houve um aumento dramático no número total de violações e ataques cibernéticos relatados nos últimos anos. Em resposta, governos e entidades corporativas investiram bilhões de dólares no financiamento de esforços de pesquisa e desenvolvimento para operações cibernéticas. Esses esforços incluem defesa da rede de computadores e ataque à rede de computadores [48]. Todas essas atividades que precedem e fazem com que as equipes cibernéticas estejam preparadas para realizar o seu trabalho, fazem parte do suporte e devem estar extremamente incluídas dentro do *cyber red team*.

A atividade de pesquisa e desenvolvimento de novas ferramentas que auxiliam enormemente o poder cibernético militar dos Estados Unidos, são uma grande prova da importância do suporte dentro do ramo militar. A agência NSA (*National Security Agency*) desenvolve diversas ferramentas, algumas disponíveis para o público, altamente úteis. Elas estão disponíveis integralmente em contas oficiais da agência dentro de sites de compartilhamento de código fonte como Github [49]. O Ghidra é um exemplo dessas ferramentas, ela inclui um conjunto de ferramentas de análise de software em baixo nível com todos os recursos que permitem aos usuários analisar

o código compilado em uma variedade de plataformas, incluindo Windows, macOS e Linux. Os recursos incluem desmontagem, montagem, descompilação, gráficos e *scripts*, além de centenas de outros recursos [50].

Em maio de 2017 iniciou-se um dos ataques de maior proporção já existente na história da computação explorando uma vulnerabilidade catalogada pela Microsoft como MS17-010, no protocolo SMB [51]. O *ransomware* [52] WannaCry atingiu com sucesso muitos hospitais, empresas, universidades e organizações governamentais em pelo menos cento e cinquenta países. Esse *ransomware* fez mais de dois milhões de vítimas, entre organizações e pessoas. O WannaCry criptografou os dados contidos em todos os computadores, com a condição de fazer o processo reverso após o resgate com pagamento em Bitcoin [53].

O poder devastador do WannaCry foi supostamente potencializado por uma dessas novas ferramentas disponibilizadas pela NSA. Esse tipo de ataque que atingiu milhões, com certeza seria de alto valor também em uma guerra [54]. Independentemente de existir ou não responsabilidades por parte da agência, a importância do suporte fica mais que comprovada.

3.2 INTERSECÇÕES DE PRIMEIRO GRAU

O conhecimento sobre as quatro competências macros, para o ambiente militar é importante, mas não é o suficiente. Para se ter uma visão mais clara e objetiva das competências necessárias para montagem de um *cyber red team* militar é preciso ir além. A partir de intersecções das quatro competências macro, é possível identificar mais quatro outras competências necessárias dentro das forças armadas, conforme ilustrado na Figura 3.2 [3].

3.2.1 Defesa ativa e passiva

A união entre as competências de ações cibernéticas e suporte, origina a competência de defesa ativa e passiva. A defesa ativa é uma ação defensiva para destruir, anular ou reduzir a eficácia das ameaças cibernéticas contra os ativos de uma organização [55]. Já a defesa passiva são todas as medidas, com exceção da defesa ativa, para minimizar a eficácia das ameaças cibernéticas [3].

Normalmente nas organizações, apenas a defesa passiva é implementada. Neste tipo de defesa, é onde aparecem os ativos como *firewalls* [56], *IPS* [57], *IDS* [58], entre outros. Apesar de ser uma atividade inerente ao *cyber blue team*, a consciência de como se fazer para contornar essas defesas implementadas, obrigam o *cyber red team* a ter o conhecimento também [3].

Para acontecer a defesa ativa e passiva dentro do *cyber red team*, além das competências necessárias de cibernética, precisa-se do suporte para implementar todas as observações nos ativos. Para um *cyber red team* é de fundamental importância que exista competências que permitam o entendimento do que acontece em relação a defesa do oponente, pois a defesa cibernética é a

barreira a ser vencida [3].

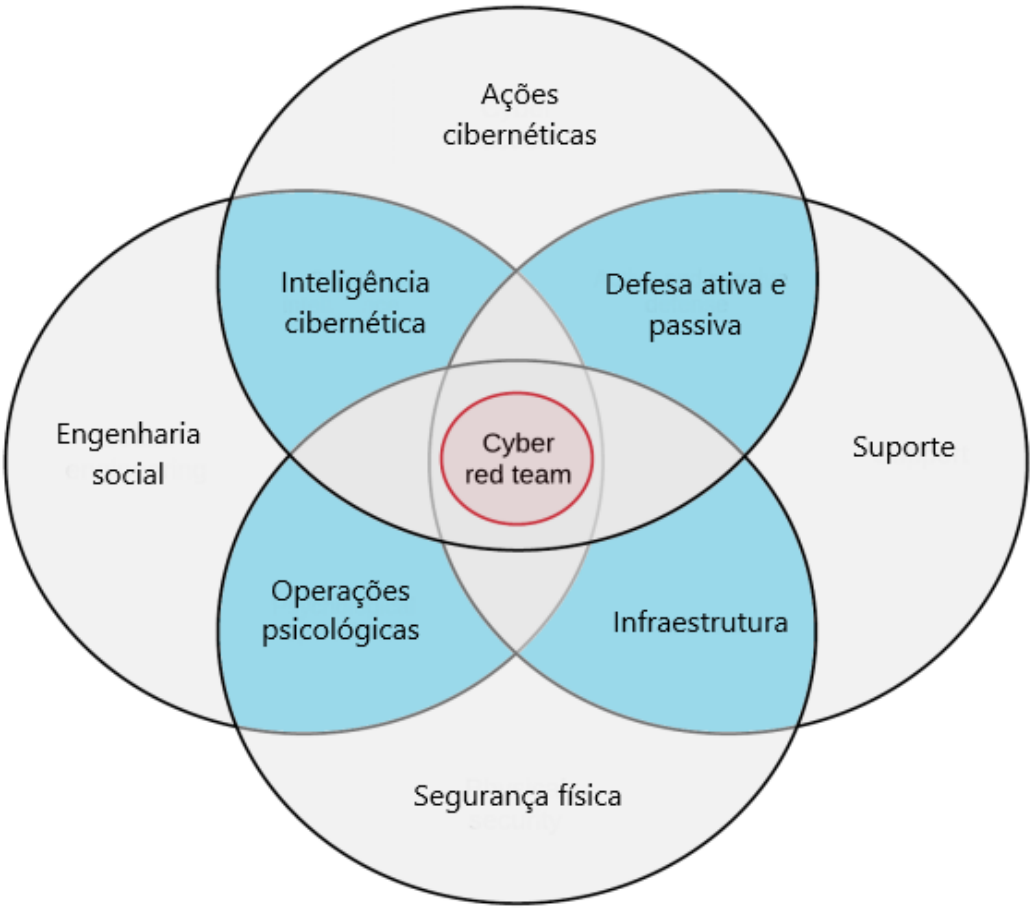

Figura 3.2: Competências por intersecções de 1º grau para um cyber red team militar.

Por exemplo, em janeiro de 2012, a organização Mitre [59] realizou o experimento de um jogo de guerra cibernética em tempo real com a utilização de *cyber teams*. Nesse exercício, foram utilizadas diversas táticas, técnicas e procedimentos. Uma das táticas empregadas pela equipe de defesa por meio do uso de uma ferramenta chamada *Blackjack* falhou e permitiu o acesso do adversário a informações no sistema da missão de comando e controle [60].

O adversário já havia comprometido várias credenciais sem o conhecimento do *cyber blue team* e, assim, acessou o sistema de missões de comando e controle. No entanto, como medida de defesa ativa e prevendo que a ferramenta poderia vir a falhar, esse sistema acessado pelo *cyber red team* era um sistema falso de missões de comando e controle. Essa técnica de defesa ativa empregada, baseada em desinformação, foi eficaz em negar o acesso do adversário as informações no sistema real de missões de comando e controle. O *cyber red team*, que era o adversário, ao obter a informação, não suspeitou que estava de posse de informações falsas e finalizou os ataques [60].

A conscientização em relação à defesa ativa é necessária para que a eficacia do *cyber red*

team não seja comprometida e o objetivo afetado. Defesa ativa é capacidade de se adiantar aos problemas que no futuro podem acontecer e trabalhar alguma medida como último recurso de proteção, muitas das vezes inesperada pelo adversário, como no caso apresentado.

Como defesa passiva, pode-se citar os *firewalls* que são ativos que protegem uma rede confiável de uma rede não confiável, filtrando o tráfego de acordo com uma política de segurança com regras especificadas. Os conhecimentos que permitem realizar ofuscações para contorno das regras pelo *cyber red team*, derivam diretamente desse conceito. A necessidade de conhecer alguns aspectos das defesas também se destina a realizar as proteções necessárias aos serviços que foram instaurados mediante exploração em um alvo [56]. Isso deve-se ao fato de resguardar o alvo capturado, já que a proteção empregada pelo *cyber red team* se destina a não permitir que ele sofra uma dupla exploração, ou seja, até mesmo, descoberto pela defesa ativa do próprio alvo. Caso isso ocorra, o objetivo imposto ao *cyber red team* seria comprometido.

3.2.2 Inteligência cibernética

A intersecção entre as ações cibernéticas e a engenharia social, origina uma competência altamente importante para as forças armadas, que é a inteligência cibernética. Com o objetivo principal de obter informações, a inteligência também se faz necessária dentro do contexto da cibernética, com mesma função [3].

A competência em inteligência cibernética é um pré-requisito para manter a superioridade no espaço cibernético [24]. Para que a captura de informações seja possível é necessário o conhecimento humano e cibernético, de forma que as informações possam ser adquiridas também de pessoas que usam este meio. Cabe ressaltar também que, a inteligência cibernética no contexto militar, não leva em consideração todas as peculiaridades de um serviço de Estado, sendo apenas para capturar informações para a própria força armada [3].

Muito usada dentro dessa competência e altamente necessária devido a utilização em massa da Internet, a OSINT(Inteligência em fontes abertas) é uma inteligência coletada e inferida a partir de fontes de informação públicas e abertas. As técnicas para realizar OSINT englobam a busca por toda informação acessível de forma pública, para facilitar esse processo ela é subdividida, pois as informações públicas são disponibilizadas de forma homógena na Internet [61]. Uma dessas subdivisões é bem utilizada devido ao alto grau de utilização das redes sociais pelo mundo, que é a OSSINT(*Open Source Social Network Intelligence*), por sua vez, possui foco na extração de informações de dados publicamente disponíveis em plataformas Web 2.0 como Twitter, YouTube e Facebook [61] [3].

Por exemplo, a Interpol [62] e outros órgãos de inteligência verificam constantemente as redes sociais em busca de suspeitos de terrorismo e também buscam prever possíveis atos para que as medidas preventivas sejam adotadas. Essa busca em meios cibernéticos serve para aprimorar os esforços de identificação e detecção em investigações nacionais de combate ao terrorismo [62].

Como exemplo dessa ação dos órgãos de inteligência, a Interpol pesquisou em plataformas

de mídia social para identificar também possíveis testemunhas, no caso após o ataque à *London Bridge* no Reino Unido em 2017. Esse mesmo ataque terrorista foi feito a um complexo hoteleiro em Nairobi, Quênia, em janeiro de 2019 [62].

Com isso, consegue-se ter uma visão mais clara sobre a importância da inteligência cibernética. Esses fatos podem ser facilmente projetados para dentro das forças armadas, pois a necessidade de busca de informação é inerentemente importante em qualquer ação de guerra e para qualquer cumprimento de objetivos por parte do *cyber red team*. Esse fato torna-a um requisito importante para o sucesso no meio cibernético.

3.2.3 Operações psicológicas

Desde a Segunda Guerra Mundial, os manuais militares norte-americanos e da OTAN definem "guerra psicológica"ou "operações psicológicas"como táticas variadas de propaganda, operações secretas, guerrilha e, mais recentemente, diplomacia pública [63]. Todas essas características podem ser utilizadas em meio cibernético também, e com o crescimento continuo das tecnologias de informação e seu uso em massa, apenas tende-se a ampliar ainda mais esse poder [64] [3].

Já sendo utilizada por boa parte das forças militares no mundo, tem-se mais uma intersecção nomeada, que deve ser competência de um *cyber red team*. Ela é a união das competências macro de engenharia social, devido a necessidade do conhecimento humano, e segurança física, pela necessidade de implante em ambiente de combate cinético [3].

As operações psicológicas são uma realidade e vem sendo aplicada em ambiente militar desde muito tempo, constituindo-se altamente importante como competência. Em meio a qualquer possibilidade de guerra a comoção e o apoio da população às operações, devem ser trabalhadas. As operações psicológicas, além de serem utilizadas contra os inimigos, também se tornam uma grande ferramenta para conquistar o próprio povo e comovê-los em relação as causas do Estado [63] [3].

Por exemplo, o Estado israelense esteve presente em luta contra o grupo terrorista Hezbollah [65]. Como parte dessa operação, foram utilizados conceitos de operações psicológicas em meios cibernéticos, o que resultou em influência nas ações do grupo inimigo [66].

As duas partes combateram no Iraque, Afeganistão e Líbano usando a cibernética ao seu favor. Tanques de guerra, aviões e soldados foram equipados com uma série de tecnologias inerente à cibernética durante as últimas duas décadas, pelo menos. Essas tecnologias aumentaram a precisão e a letalidade do armamento, a percepção situacional do soldado e a eficiência geral das operações [66].

No entanto, em 2007 em meio ao conflito, um fenômeno cibernético estava em evolução e já era conhecido: o conceito de operações ciber-psicológicas - que são operações cibernéticas que visam atacar e influenciar diretamente as atitudes e comportamentos dos soldados inimigos ou até mesmo toda a população. Enquanto os exércitos continuavam empregando seus esforços em uma

guerra cibernética que acontecia, a população estava sendo vítima de ataques de influência digital [66].

As operações ciber-psicológicas (CYOP) também trazem consigo consequências não intencionais, decorrentes do grau de emprego do poder de influência, persuasão, engano e mobilização que o ambiente cibernético oferece [66].

Mediante a utilização dos meios de cibernética para aplicação também dos conceitos de guerra psicológica e devido aos seus resultados proporcionarem favorecimento a quem emprega, torna-se uma competência necessária ao *cyber red team* militar. O emprego dos fatores inerentes a uma operação psicológica pode influenciar diretamente a eficiência de um *cyber red team*, principalmente em meio a uma guerra cibernética, onde vidas estão em risco.

3.2.4 Infraestrutura

Da intersecção da segurança física com a área de suporte surge a competência de infraestrutura, uma área essencial para a cibernética. Todo o setor de infraestrutura de tecnologia da informação e da comunicação (TIC), é altamente necessário para o emprego dos *cyber red teams*, pois sem ele não tem cibernética. Esse setor é composto por diversas áreas de conhecimentos como redes, servidores, banco de dados, manutenção de ativos, sistemas operacionais e *hardwares* [67] [3].

A infraestrutura é como uma rede, com sistemas e processos independentes, que normalmente é de propriedade privada. São criadas pelo homem e funcionam de forma colaborativa e sinérgica, para produzir e distribuir um fluxo contínuo de bens e serviços essenciais [68]. Isso significa que, o detentor dessa infraestrutura, ou até mesmo alguém que consiga explorar e tirar proveito, pode executar ações sobre diversas informações. Com essa afirmação, torna-se claro que infraestrutura está dentro das competências de segurança física e suporte e altamente vinculado as ações esperadas por um *cyber red team* [3].

Por exemplo, em 23 de dezembro de 2015, a empresa ucraniana Kyivoblenergo, de distribuição de energia, relatou interrupções no serviço aos seus clientes [69]. As interrupções ocorreram devido à entrada ilegal de terceiros no computador e nos sistemas *SCADA* da empresa. Sete subestações foram desconectadas por três horas. Declarações posteriores indicaram que o ataque cibernético impactou partes adicionais da rede de distribuição e obrigou os operadores a mudar para o modo manual. O evento foi apurado pela mídia ucraniana, que realizou entrevistas e determinou que um atacante estrangeiro controlava remotamente o sistema de gerenciamento de distribuição [69].

Logo após o ataque, oficiais do governo ucraniano alegaram que as interrupções foram causadas por um ataque cibernético e que os serviços de segurança russo foram responsáveis pelos incidentes [69]. Após essas alegações, investigadores na Ucrânia, bem como empresas privadas e o governo dos EUA, realizaram análises e ofereceram assistência para determinar a causa raiz da interrupção [69].

Esse exemplo exibe a importância de conhecer os tipos de infraestruturas e suas peculiaridades. Infraestruturas críticas são fundamentais para um pais, pois possuem serviços que, sua falta, pode ocasionar uma situação caótica [70]. Os *cyber red teams* devem possuir conhecimento aprofundado sobre infraestruturas críticas para que possam oferecer riscos ao inimigo e também para que possam treinar o *cyber blue team* para defender algo tão vital.

3.3 INTERSECÇÕES DE SEGUNDO GRAU: AS MAIS PRÓXIMAS DO *CYBER RED TEAM*

Da análise feita em torno das competências até esse momento, chega-se à existência de quatro competências macros e mais quatro, originadas de intersecções. Ao total tem-se oito competências identificadas para um melhor mapeamento de um *cyber red team* no contexto militar. No entanto, o que foi listado até agora, ainda não demonstra claramente todas as competências necessárias. Pode-se, por exemplo, detalhar mais um pouco as intersecções, de forma a chegar, em competências mais próximas as necessidades do *cyber red team* militar, conforme ilustrado na Figura 3.3 [3].

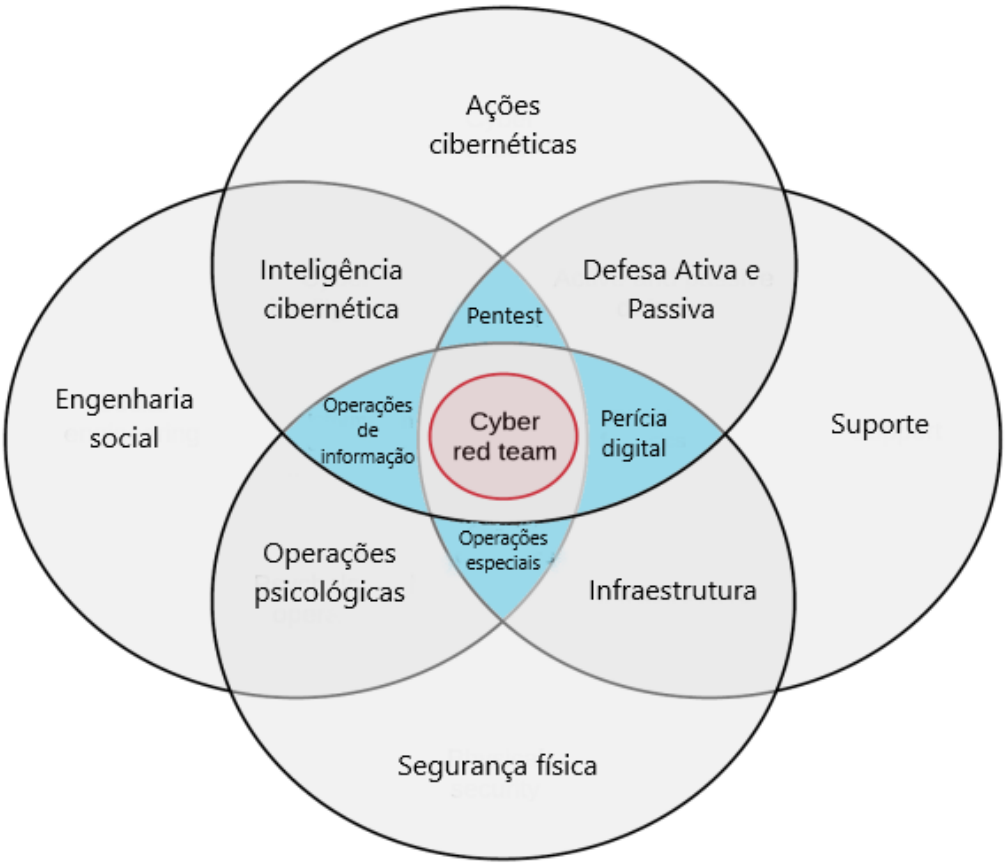

Figura 3.3: Competências por intersecções de 2º grau para um cyber red team militar.

3.3.1 Testes de penetração (*pentest*)

Conforme já dito anteriormente, diferentemente do processo de teste de penetração (*pentest*), um *cyber red team* não visa encontrar o maior número de vulnerabilidades possíveis e sim, conquistar um objetivo imposto. Porém, não se tem um *cyber red team* sem os profissionais de *pentest*, os quais são partes integrantes [3].

Metodologias de *pentest*, como, por exemplo, o PTES (*Penetration Testing Execution Standard*) preveem fases de reconhecimento passivo e ativo, exploração de falhas, preservação do acesso e geração de relatórios [8]. Os resposáveis pelo *pentest* devem utilizar as mais variadas técnicas, inclusive aprender com crimes digitais como, por exemplo, as fraudes bancárias, onde existem formas criativas e inovadoras para realizar ataques [71] [3].

Essas atividades, devem ser incorporadas dentro do *cyber red team*. Ela é claramente uma união das competências de inteligência cibernética, pelo fato de possuir fases de reconhecimento, e da defesa ativa e passiva, por ter que interagir com o meio. Também considera a forte ação das competências macro de engenharia social, ações cibernéticas e suporte, que são em alto nível incluído nas atividades de *pentest* [3].

Por exemplo, a Cylance, em [10], publicou um estudo de caso, que relata a existência de um grupo que se apresentava em forma de uma empresa de segurança, mas na verdade era uma farsa. Esse grupo operava abertamente como uma empresa de segurança e oferecia serviços de proteção. Algumas evidências descobertas sugeriam que, embora essa empresa fosse respeitada por alguns clientes, provavelmente também era responsável por extrair mais de duzentos megabytes de dados sensíveis de um sistema de controle de tráfego aéreo. Esses dados foram encontrados, posteriormente, em um repositório de *malware* semi-público.

Essa mesma equipe, camuflada também em forma de empresa de *pentest*, foi capaz de afetar aeroportos, organizações de assistência médica, grandes instituições financeiras, grandes empresas de tecnologia, governos estaduais e locais, organizações sem fins lucrativos globais, grandes varejistas e agências governamentais federais dos EUA. Tudo isso foi revelado por meio das análises feitas sobre os *malwares* e *phishings* capturados e apresentados no estudo [10].

Diversos *malwares* gerados pela equipe e também outras ferramentas que foram projetadas para uso dos *cyber blue teams* agora estão nas mãos de vários atores, envolvidos com crime organizado direcionados a Estados [10].

Isso deixa uma dúvida em relação à confiabilidade dos serviços de segurança. Neste caso, coloca sobre os órgãos de Estado uma responsabilidade a mais, até mesmo na hora da contratação de um serviço de segurança. Com isso, torna-se obrigatório que as forças armadas, que não podem ficar a mercê de qualquer empresa, estarem preparadas para executar as mesmas operações e conhecer todos os aspectos relativos aos *pentests*. Claramente se torna uma competência necessária ao *cyber red team* militar.

3.3.2 Operações de informação

Para que se possa moldar o ambiente de informação, de acordo com os interesses, é preciso o desenvolvimento de operações de informação, inclusive em redes de computadores. Com isso, deve-se potencializar, os ditos, "pontos fortes"na exploração e reduzir o máximo possível os impactos dos ataques que pretendam explorar os "pontos fracos"[72] [3].

Com base no exposto, existe uma competência que surge da intersecção da inteligência cibernética com as operações psicológicas. E para isso não descarta a interferência direta das três habilidades macro: engenharia social, ações cibernéticas e segurança física . As operações de informação exigem uma forma interdisciplinar e complexa e é usada para obter informações negada de alta dificuldade [73] [3].

As operações de informação surgem dentro do *cyber red team* pela sua necessidade de obter informações negadas. Essas informações que devem chegar ao *cyber red team* são valiosas e o valor é independente da forma com que foi obtida. A grande vantagem das operações de informação é que com ela se tira proveito das ações feitas fisicamente mediante persuasões ou outros métodos e também de forma cibernética [73] [3].

Por exemplo, o uso da Internet por terroristas pode ser classificado em duas categorias: comunicação e instrumental [74]. O primeiro compreende a disseminação da propaganda, a realização de campanhas de guerra e mobilização de membros potenciais do grupo, enquanto que o último inclui doutrinação e treinamento, planejamento cibernético e coordenação, bem como captação de recursos [75].

A estreia online da Al-Qaeda ocorreu em fevereiro de 2000, com a criação do site "maalemaljihad.com", seguida em março de 2001 pelo "alneda.com". Em seguida, sua URL passou a ser regularmente modificada. Eles eram sempre forçados a mudar de servidor para servidor pelas denúncias dos cidadãos. Depois de perder o domínio da Internet em 2002, a Al-Qaeda reapareceu mais tarde com um novo site chamado Faroq [75].

A organização terrorista reconhece explicitamente a importância da Internet como ferramenta de propaganda e pede contribuições para sua abordagem geral de comunicação, como fez em um de seus inúmeros sites. De posse desse meio, consegue montar complexas atividades, que envolve cibernética e ações físicas, todo seu trabalho conta com a Internet, como meio de divulgação e captação de recursos.

Para desmantelar o trabalho de terrorismo os Estados mais afetados desenvolvem complexas operações de informação, para apoio. Essas operações utilizam de todos os meios possíveis para saber tudo sobre as ações das organizações criminosas, sendo um complexo sistema baseado em preceitos de inteligência, cibernética e psicologia. A denúncia da população aos órgãos é de extrema importância, por isso a operação de informação engloba uma multidisciplinaridade imensa [76].

Como tudo isso, as operações de informação tornam-se altamente necessárias para o *cyber red team*. Isso para que a equipe cibernética tire proveito dos conhecimentos retirados desse tipo de

operação e que também seja capaz de colaborar com o Estado de forma eficiente, quando incluída na mesma.

3.3.3 Operações especiais

Ao levar em conta a possibilidade de um confronto, um *cyber red team*, mesmo sendo ele focado em cibernética, deve estar preparado para obter informações provenientes de combate físico. Para isso, é necessário que membros do *cyber red team* sejam capazes de permear esse meio [3].

Com isso, origina-se uma intersecção, com grau de probabilidade para utilização que pode ser considerado baixo para os *cyber red teams*, porém, importante e que deve estar na lista de habilidades necessárias. A junção das operações psicológicas com a infraestrutura, com grande influência das competências macro de engenharia social, suporte e principalmente segurança física, gera a competência de operações especiais [3].

Percebe-se que à medida em que as operações de influência vão se afastando do campo das operações psicológicas e aproximando-se de ações paramilitares e guerrilha, as operações especiais entram em ação com as tropas de elite [77]. Por isso, torna-se necessário o mapeamento das operações especiais como competência, mesmo que sua utilização seja de baixa probabilidade, sendo usada, apenas nos níveis avançados de combate ou de exercício [3].

Por exemplo, a demanda por recursos holandeses para operações especiais está em constante aumento [78]. O período pós onze de setembro, acarretou em missões militares especiais das tropas holandesas no Afeganistão, Iraque, Somália, Mali e outros países não ocidentais. Isso juntamente com a instabilidade expandida na Europa Oriental como resultado de ações russas, foram combinadas com a crescente demanda por tarefas nacionais para operações especiais. Esse fato foi potencializado devido as possibilidades de ações terroristas no país que aumentaram a demanda por militares holandeses [78].

A partir dessas ações foi percebido que as tropas de operações especiais holandesas poderiam operar sob diferentes circunstâncias. As tropas poderiam explorar, defender e atacar pessoas, dados, informações, sistemas e inteligência para conscientização situacional nacional, apoio moral e social no domínio físico e, eventualmente, no virtual [78]. Isso porque, alguém preparado em meio a essas tropas pode retirar informações de meios cibernéticos isolados e usar essas mesmas informações no futuro.

Os papéis futuros das tropas de operações especiais holandesas podem ser a formação e preparação do contexto estratégico e incluir os recursos cibernéticos [78]. Nesse contexto estratégico, existe uma grande integração entre as guerras cinética e cibernética, onde esses conflitos híbridos são considerados a "norma"e o comportamento humano é a "chave"[79].

Com isso a Holanda passaria a reconhecer a importância de uma ação hibrida, entre operações especiais e cibernética. Isso traz para dentro do *cyber red team* a necessidade de possuir profis-

sionais que estejam preparados para acompanhar tropas especiais a fim de obter informações em redes isoladas ou até mesmo em computadores.

3.3.4 Perícia digital

Como última intersecção definida antes de se chegar ao fechamento das habilidades necessárias ao *cyber red team*, está a competência que dispensa a interação direta com o ser humano, mas é essencial. A perícia digital é a intersecção das habilidades em infraestrutura com as atividades de defesa ativa e passiva [3].

Essa competência também conta com forte influência dos macros operações cibernéticas, segurança física e suporte. Para que uma perícia aconteça deve haver segurança no armazenamento dos dados, conhecimentos de cibernética para que a coleta seja feita e um grande aparato de suporte, com máquinas de poder computacional considerável para quebras de senhas e processamento de *hashs* [80] [3].

Em um *cyber red team* é de fundamental importância a competência em perícia digital para permitir a extração de dados de meios computacionais, inclusive em dispositivos móveis [81]. Também deve ser conhecida para que os componentes do *cyber red team* possam aplicar a anti-perícia. Com isso o trabalho feito pelo *cyber red team*, torna-se de mais difícil rastreamento [3].

A perícia é necessária, pois com ela se tem acesso a informações que a priori são tidas como apagadas ou inexistentes. O fato de se conhecer as maneiras de recuperar dados e reconhecer ações feitas anteriormente potencializam também as habilidades da anti-perícia, já que dessa forma o *cyber red team* irá saber se suas ações podem ser rastreadas pelo inimigo [82] [3].

Por exemplo, no ano de 2016 [83], a então primeira-dama do Brasil, Marcela Temer, relatou que foi chantageada por um homem que usou os seus serviços do *iCloud* e *WhatsApp*, para obter dados sigilosos. A pessoa que a chantageava supostamente adquiriu um Disco rígido, de sua antiga posse, em um bairro da cidade de São Paulo chamado de Santa Ifigênia no valor de duzentos e cinquenta reais[83]. A partir desse disco rígido, foi possível recuperar informações que indicavam a existência de dados pessoais, da então primeira-dama, no banco de dados de um provedor. Esse fato, explicou a forma utilizada para aquisição de dados não autorizados que possibilitaram o acesso as contas dos serviços, pelo suposto criminoso[83].

O suspeito, então, foi acusado de solicitar a primeira-dama uma quantia de trezentos mil reais, para não divulgar prováveis fotos íntimas, e também áudios comprometedores que estavam supostamente sobre sua posse. Esses dados, pelos indícios, foram obtidos por meio de recuperação de arquivos do seu Disco rígido e também pelos sucessivos acessos as contas em serviços de armazenamento de dados online, como no caso o *Icloud* [84].

Além disso, uma das afirmações possivelmente feita pelo suspeito, é que ele estaria de posse também de evidências que poderiam ser usados contra o então presidente do Brasil, Michel Temer

[85]. Independentemente de juízo de valores sobre o caso, qualquer situação envolvendo autoridades importantes, ainda mais sendo ela o presidente de república, pode causar instabilidade econômica, política, revoluções, entre diversas outras consequências.

As atividades relativas à perícia digital, ou também conhecida como forense digital, devem ser habilidades presentes no *cyber red team*. Torna-se necessário extrair informações de meios físicos originados de combate cinéticos, mesmo que danificados ou, até mesmo, realizar todos os procedimentos para retirar informação apagada de um computador remoto. Tudo isso envolve o conhecimento de perícia digital.

Além do mais, análise de *malware* e suas ações podem acarretar em grandes vantagens cibernéticas, pois falhas no desenvolvimentos de armas cibernéticas podem resultar em vantagens contra o inimigo [86]. Com todo esse conhecimento, também é possível empregar os meios para o aumento da eficiência e ofuscação dos ataques feitos pelo *cyber red team*.

4 METODOLOGIA DE TREINAMENTO CONTÍNUO

A metodologia de treinamento contínuo desenvolvida neste trabalho não exige que os profissionais se envolvam exclusivamente nos exercícios, mas permite um aumento constante das suas habilidades exigidas em ações cibernéticas militares. Para implementar a metodologia na prática, também é necessário atender aos pré-requisitos e redes usados pela metodologia.

O sucesso da metodologia que será apresentada nesta dissertação depende fortemente das equipes que participarão. Por isso, é altamente recomendado que as equipes sejam montadas de acordo com as habilidades citadas neste trabalho. Em casos diferentes, pode-se, até mesmo, obter uma melhora nas equipes, no entanto, não será extraído todo o potencial que a metodologia proposta proporcionará para o aumento contínuo das habilidades cibernéticas. Esse fato como consequência trará um impacto menor na projeção do poder militar na guerra cibernética.

4.1 PRÉ-REQUISITOS

Para implementar a metodologia de treinamento contínuo, a organização militar deve ter uma política de segurança forte que permita a criação de três equipes cibernéticas. Essas equipes cibernéticas são o *cyber red team* para ações ofensivas, o *cyber blue team* para ações defensivas e o *cyber purple team*, que pode ser uma equipe pequena, composta por dois profissionais.

O *cyber blue team* é uma equipe que normalmente já existe nas instituições militares, mesmo que não conhecida com esse nome, pois é a equipe que realiza a defesa cibernética e todo o processo de segurança da informação [87]. De um modo geral, o *cyber blue team* já possui as permissões necessárias para seu correto funcionamento. O *cyber red team* é também muito conhecido em ambiente militar, pois é a equipe que deve estar preparada par realizar as ações ofensivas da força militar [88]. Essa equipe deverá possuir as permissões necessárias para realizar operações ofensivas na instituição.

Já o *cyber purple team*, pode ser tido como algo novo, pois é uma equipe gerenciadora de exercícios, os quais são bases para essa metodologia. O *cyber purple team* deverá ter permissão para gerenciar a infraestrutura e direcionar os exercícios para atender aos objetivos. Essa equipe deve ser conhecida por todos, isso inclui os seus próprios membros. Também devem ser treinadas nas tecnologias usadas na organização e totalmente respaldada pelo comando estratégico, para isso precisam ter conhecimento documentado de tudo, que envolve cibernética na organização.

A organização deve ser capaz de prover os recursos de infraestrutura necessários para clonar duas vezes a mesma rede de serviços e suas dependências. Não é necessário que exista recursos para prover tudo de forma simultânea, no entanto, deve haver recursos pelo menos para clonar a rede de serviços que o *cyber purple team* definiu como destino dos testes.

O *cyber blue team* deve ser capaz de distinguir o que acontece nas redes de exercícios do que acontece na rede de produção. Por isso, deve existir uma segregação clara entre as redes. Com isso, o *cyber blue team* poderá atribuir prioridade inferior aos eventos que acontecem fora do ambiente de produção. Essa ação permitirá que o exercício ocorra de modo contínuo e não interfira no trabalho real.

4.2 *CYBERANGE* DE TRABALHO

O primeiro passo para criação de um *Cyberange* é replicar uma rede já existente na organização. Com o *Cyberange* é uma rede segregada como o objetivo de suportar os testes de segurança de forma isolada, a nossa rede clonada deve ser escolhida com base nesse objetivo. Para esse fim, A figura 4.1 exemplifica uma infraestrutura total, que pode ser utilizada por uma organização militar e dela será retirado a rede base para um *Cyberange*.

Criar um *cyberange* envolve diversas ações auxiliares além da clonagem, disponibilização e segregação de uma infraestrutura para os exercícios. Planejar um bom *cyberange* envolve criar uma arquitetura em camadas que permita integração entre as equipes e os ativos, que representa também o ambiente real com uma gama possível de vulnerabilidades cibernéticas. Além disso, ferramentas para registro dos dados de ataque para treinamento e análise adicionais devem estar implementadas [89].

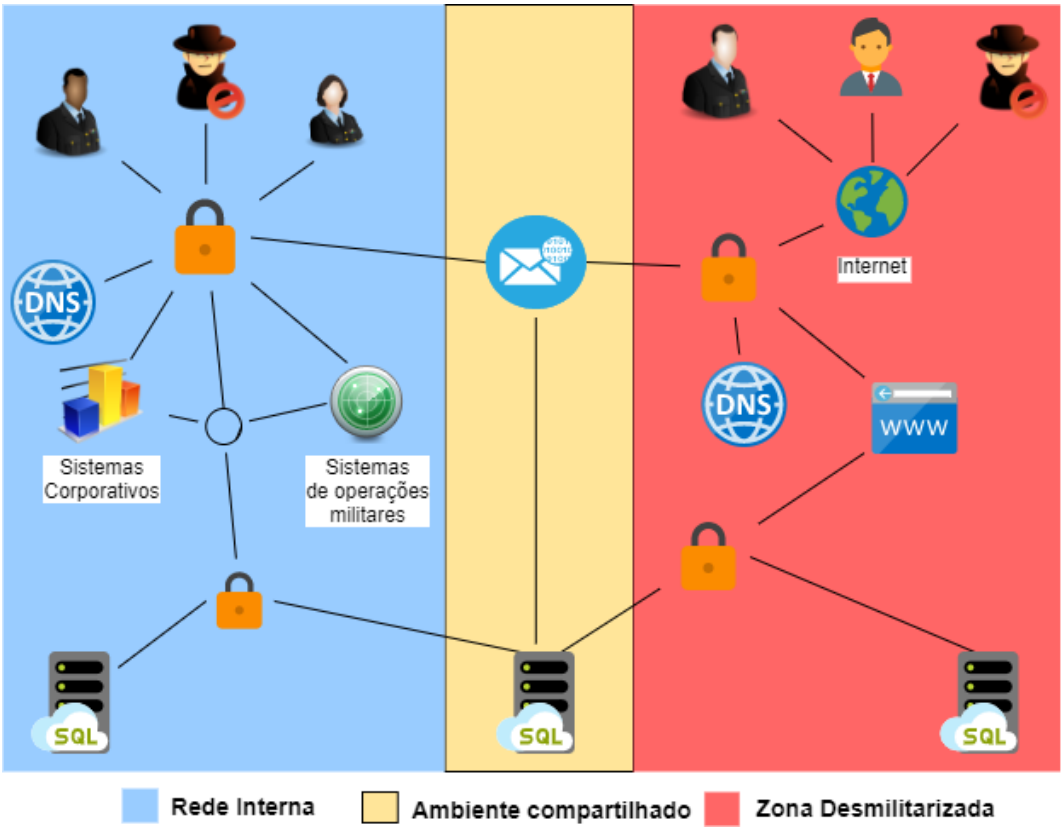

Figura 4.1: Exemplificação de infraestrutura da rede militar

A metodologia proposta trabalha com três redes diferentes em paralelo. Sendo uma delas, a rede de produção, a qual também é considerada como parte integrante, no entanto se mantém fora do *cyberange*. Cada uma das redes tem seu objetivo e, juntas, constituem o ambiente necessário para a eficiência da metodologia. A rede experimental é usada para o desenvolvimento de ataques cibernéticos e o conhecimento gerado é transferido para a rede de exercícios, onde o *cyber blue team* aprende a vulnerabilidade executada e implementa a correção na rede de produção.

Em resumo, a rede experimental não possui monitoramento ativo pelo *cyber blue team*, apenas as defesas já implementadas previamente. Isso faz com que apenas o *cyber red team* atue diretamente nessa rede. Na rede de exercícios, o *cyber red team* e o *cyber blue team* agem com força total e as medidas de desempenho são feitas pelo *cyber purple team*. O *cyber purple team* gerencia toda a infraestrutura de rede, com exceção da rede de produção que é gerenciada pelo *cyber blue team*. A Figura 4.2 exibe de modo figurativo as redes existentes e as ações que todas as equipes realizam nela.

4.2.1 Rede experimental

A rede experimental é uma cópia de uma rede de produção. Essa rede é usada para o desenvolvimento de ataques cibernéticos e o *cyber blue team* não possui monitoramento. Por isso que a seta do *cyber red team* na Figura 4.2 está marcada na cor verde, quando apontada para rede experimental. A seta do *cyber blue team* que é apontada para rede experimental, está marcada na cor amarela. Isso indica que toda a ação *cyber red team* na rede, deve ser feita com total liberdade. Já a ação do *cyber blue team* é limitada, porque apenas as defesas anteriormente implementadas devem estar ativas. Essa cópia da rede de produção não deve incluir os ativos que proporcionam ao *cyber blue team* o monitoramento da rede.

A rede experimental é uma rede exclusiva para uso do *cyber red team* e para construir essa rede, o *cyber purple team* deve selecionar uma rede de produção e clonar todos os ativos que a compõem, incluindo *firewall*, *WAF* [90], *IPS*, *IDS*, entre outros. Não é necessário clonar ativos de monitoramento na rede experimental, mas se tiver sido clonado, não deverá estar ativo, de forma a enviar informações da rede para o *cyber blue team*.

O *cyber purple team* deve bloquear na rede experimental todas as comunicações para o *cyber blue team* e permitir que a rede seja exclusiva do *cyber red team* para desenvolver seus ataques cibernéticos. Nela, o *cyber purple team* pode implementar os seus ativos de controle, para que as informações relativas ao andamento do desenvolvimento dos ataques sejam metrificadas.

Uma vez que o *cyber red team* envie um comunicado ao *cyber purple team* para informar que o ataque cibernético está pronto para ser executado em ambiente de exercícios, o *cyber purple team* dará prosseguimento nos passos da metodologia. Para isso, ele deverá enviar um aviso ao *cyber blue team*, de que haverá a ativação de um ambiente de exercício. Com isso será ativada a rede de exercícios, que pode ou não ter sido criada com antecedência.

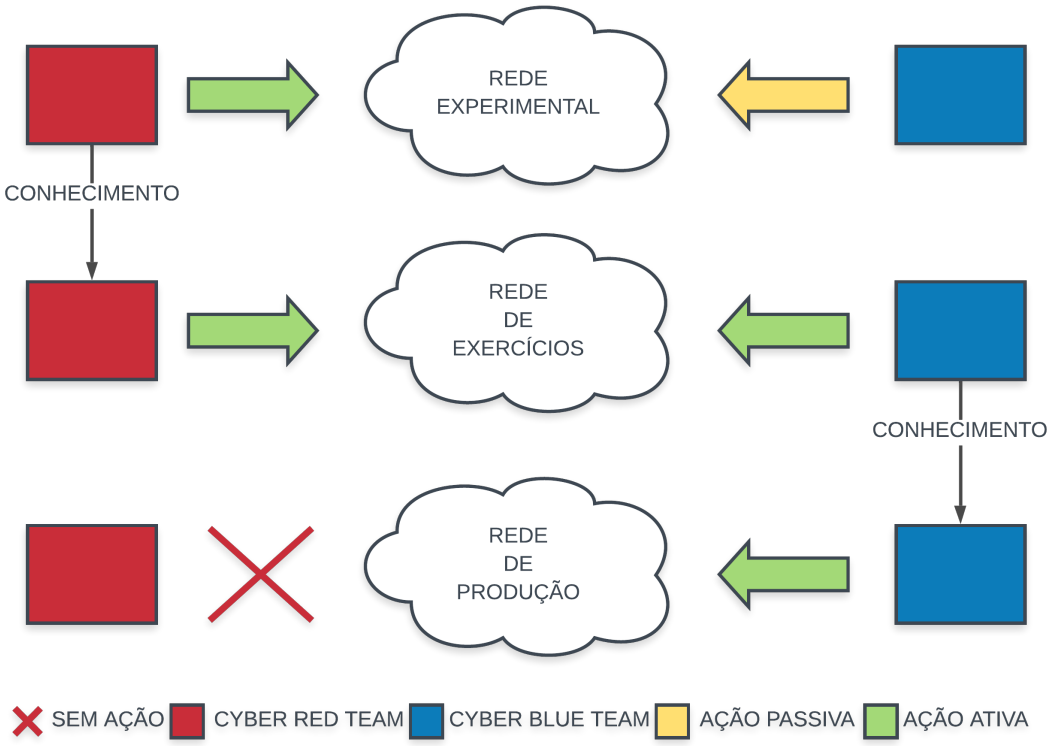

Figura 4.2: Modo de operação dos *cyber teams* nas redes propostas pela metodologia

Como exemplo de uma rede copiada, tem-se a Figura 4.3. Essa rede foi elaborada a partir da cópia de parte dos serviços expostos na infraestrutura total, apresentada na figura 4.1. Note que todos os ativos copiados para essa rede experimental possuem interação entre si, ou seja, compõem a totalidade do serviço. No caso apresentado, é o sistema de concursos e os ativos relacionados são os de segurança, o de resolução de nomes, o banco de dados e o servidor WEB do próprio sistema.

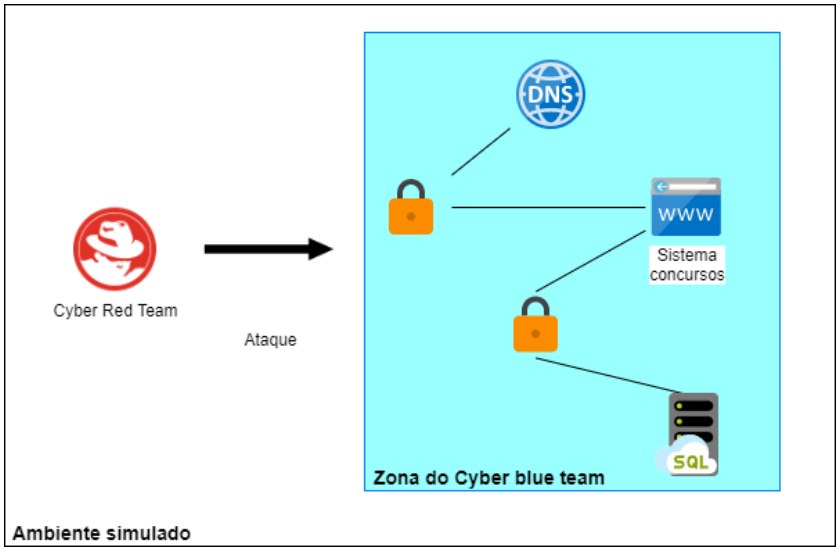

Figura 4.3: Rede Experimental de exemplo

4.2.2 Rede de exercícios

A rede de exercícios é uma cópia exata da rede de produção, diferentemente da rede experimental, que não inclui a ação dos ativos de monitoramento de rede. Com isso, a rede de exercícios é uma simulação real do ambiente ativo na organização. Nessa rede ocorrem os ataques cibernéticos que foram desenvolvidos anteriormente pelo *cyber red team* na rede experimental. Por isso, nela os ataques e a defesa podem ser avaliados como se em emprego real estivessem.

Na rede exercícios é possível avaliar com maior precisão a eficácia e a eficiência de ambas as equipes, que realizam os ataques e a defesa. Nesta rede, o *cyber red team* e o *cyber blue team* agem com toda a capacidade que têm disponível no momento, sem se preocuparem com os danos colaterais que uma ação pode acarretar. Como esta rede é a simulação do ambiente real de atuação, o *cyber blue team* deve monitorar todas as atividades e deve se esforçar para interromper os ataques. É por isso que na Figura 4.2 as duas equipes têm uma seta verde.

Diferente da rede experimental, na rede de exercícios, o ataque deve estar pronto para o emprego e funcional, com a sua eficácia provada na rede experimental. Um erro do *cyber red team* pode custar o objetivo, não atingindo-o devido às barreiras implementadas. E caso isso ocorra, o *cyber blue team* é dado com vencedor da batalha.

A rede de exercícios deve ser paralela à rede de produção, assim como também a rede experimental, e a prioridade de seus eventos não deve ser maior que a rede de produção, para evitar ataques reais no momento dos exercícios. Essa premissa, permite o treinamento contínuo em conjunto com o trabalho sem exigir dedicação exclusiva.

A função do *cyber purple team* na rede de exercícios é cria-lá e também gerenciar os fatos inerentes ao controle das equipes. Nesta rede, o *cyber purple team*, caso julgue necessário, pode determinar pontos de início para o ataque, que vão além da realização de todo o processo. Isso é para permitir que a eficácia das camadas mais superiores de defesa, inibam o teste das camadas mais inferiores. Com isso, permite-se que as defesas sejam avaliadas em ataques que partem de pontos não previstos, muito comuns após uso de engenharia social [43].

A rede de exercícios é a principal rede da metodologia, nela, o *cyber purple team* deve ser capaz de extrair o maior número de dados estatísticos possíveis. Esses dados coletados na rede, serão usados posteriormente para análise das habilidades e também para maior direcionamento dos exercícios em campanhas futuras. Isso permitirá o incremento de pontos deficitários ou que podem ser melhorados dentro das habilidades de ambas as equipes.

4.2.3 Rede de Produção

A última rede é a produção, onde o *cyber blue team* implementa o conhecimento gerado na rede de exercícios e o *cyber red team* não tem ação. Essa rede pode ser conhecida por demais nomes como, rede de trabalho real, rede de operação, etc. Essa nomenclatura apenas depende da referência utilizada.

A rede de produção consiste na rede em que uma organização realmente aloca os seus serviços para serem disponibilizados para utilização de seu público final. Ela contêm os mais variados tipos de serviços que possuem valor para organização [91].

Depois que o *cyber blue team* implementa as configurações e ferramentas necessárias para corrigir as falhas descobertas nos exercícios na rede de produção, ela já pode ser clonada novamente em uma rede experimental. Essa ação, não precisa ser feita imediatamente, no entanto, em algum momento será feita, pois é essa ação que caracteriza o ciclo de treinamento contínuo, onde o nível de dificuldade aumenta conforme o tempo.

Após o *cyber red team* explorar as vulnerabilidades na rede de exercícios e o *cyber blue team* realizar os reparos na mesma rede, essas mudanças serão realizadas na rede de produção. Ou seja, a correção será implementada na rede de exercícios, para que seja provada sua eficácia. Isso diminui a probabilidade de ser realizado um esforço falho na rede de produção.

À medida que as defesas serão aprimoradas, o monitoramento também será aprimorado. Portanto, para que novos ataques na rede experimental e na rede de exercícios sejam exibidos, eles devem seguir a rede de produção.

4.3 FLUXO METODOLÓGICO

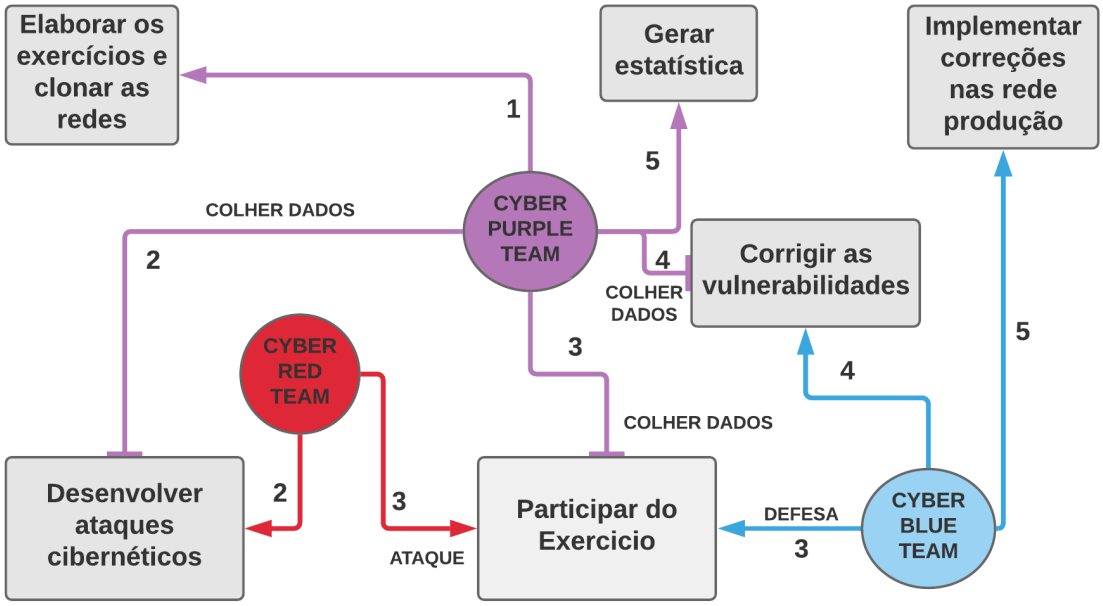

Figura 4.4: Fluxo de atividade dos *cyber teams*, de acordo com a metodologia proposta.

A Figura 4.4 ilustra o fluxo da metodologia proposta, na qual as cores representam cada equipe definida neste trabalho. A numeração indica a ordem com que a ação acontece dentro da metodologia e, como pode ser percebido, algumas ações contêm a mesma numeração. Isso indica que

essas ações fazem parte do mesmo passo e acontecem em paralelo, pois são realizadas por equipes diferentes. As caixas cinzas são as representações das ações possíveis dentro da metodologia proposta e as linhas indicam as equipes que participam dessas ações. No caso das linhas com seta, o significado é uma ação ativa da equipe e a linha com final achatado, indica que a ação é passiva.

A tabela 4.1, descreve de forma resumida os passos que estão listados na Figura 4.4. A partir disso pode-se ter um conhecimento direto das atividades que são realizadas por cada *cyber team* em cada passo descrito na metodologia proposta.

Tabela 4.1: Resumo dos passos do fluxo por *cyber teams*

Passos	***Cyber purple team***	***Cyber red team***	***Cyber blue team***
1	Elaborar exercícios e clonar as redes.	X	X
2	Colher dados	Desenvolver ataques cibernéticos	X
3	Colher dados e monitorar	Realizar o ataque	Realizar a defesa
4	Colher dados	Homologar defesa	Desenvolver a correção da falha
5	Gerar estatística geral	X	Corrigir na rede de produção

4.3.1 1º Passo: Montar a infraestrutura

O primeiro passo para dar início às ações da metodologia é decidir qual infraestrutura deve ter seus sistemas de defesas levados à prova. Isso é função da alta gestão [42] que por sua vez, tem ciência das melhorias necessárias para melhor projeção do poder militar e capacidade de defesa cibernética. A execução dessas ações dentro da metodologia cabem ao *cyber purple team*.

Após a expressão das necessidades da alta gestão ao *cyber purple team*, a equipe deve realizar as comunicações necessárias e providenciar o atendimento do requisito imposto. O *cyber purple team* é a equipe responsável por clonar a rede de produção, conforme as necessidades de testes, em duas redes diferentes. Essas redes são a rede experimental e a rede de exercícios, mas não

é necessário que esse clone seja feito de forma imediata ou simultânea, pois o primeiro foco é a rede experimental.

Como já mencionado anteriormente, a rede experimental e a rede de exercícios devem ser idênticas à rede de produção, no entanto, na rede experimental, a funcionalidade de monitoramento pelo *cyber blue team* não deve estar ativa. Então, no momento em que for feito o clone de uma rede de produção para rede experimental, o *cyber purpe team* deve-se atentar no detalhe de não permitir a comunicação dos ativos de monitoramento com o *cyber blue team*.

Em relação ao tempo para desenvolvimentos dos ataques pelo *cyber red team*, o *cyber purple team* deve definir um limite de tempo. Esse tempo pode variar de acordo com o nível das equipes ou a necessidade da organização. Isso para que não seja aplicado um esforço extra em atividades de probabilidade muito baixa, onde poucas chances de encontrar vulnerabilidades são vistas. Com essa ação consegue-se direcionar o esforço do *cyber red team* para situação mais plausíveis. Essa situação pode ser alterada, a depender o nível de capacidade que se encontra o *cyber red team* e o objetivo pretendido.

4.3.2 2º passo: Desenvolvimento dos ataques

Quando a rede experimental estiver totalmente funcional, o *cyber purple team* deve enviar um comunicado ao *cyber red team* que, por sua vez, deve começar a desenvolver ataques cibernéticos na rede. No entanto, para que o desenvolvimento dos ataques tenha um sentido, também é necessário definir objetivos e metas a serem alcançadas pelo *cyber red team*.

O objetivo para o *cyber red team* também deve ser baseado nas necessidades expostas pela alta gestão, pois em uma situação real de guerra é a alta gestão do comando militar que norteará as informações necessárias à organização [15]. Como é um treinamento, a fim de ampliar a capacidade de projeção de poder militar em uma guerra cibernética, deve-se obedecer a mesma cadeia hierárquica. Esses objetivos podem ser dos mais variados tipos, desde apenas a busca por uma informação negada até mesmo modificação ou negação de serviços em infraestruturas críticas.

Depois que o *cyber red team* atingir o objetivo que lhe foi imposto na rede de experimentos, por meio do desenvolvimento de um ataque cibernético, esse mesmo ataque deve ser replicado na rede de exercícios. Para isso, o *cyber red team* deve comunicar o *cyber purple team* que já existe um ataque funcional e que está tudo preparado para testar as defesas em um ambiente com monitoramento real. Essa notificação deve ser feita, para que o *cyber purple team*, caso ainda não tenha feito, faça a estruturação da rede de exercícios e também finalize os dados que resultam em métricas, na rede experimental.

Na rede experimental, por meio da resposta do *cyber red team* sobre a conclusão do desenvolvimento do ataque cibernético para rede, o *cyber purple team* calculará o Tempo de Desenvolvimento de Ataques (TDA). Essa métrica é usada para acompanhar o desempenho do *cyber red team*.

4.3.3 3º passo: O exercício

Na rede de exercícios, o *cyber blue team* age com o mesmo poder que tem na rede de produção, ou seja, todo. No entanto, aos alertas de ataques nas ferramentas de monitoramento deve-se atribuir uma prioridade mais baixa ao tráfego oriundo da rede de exercícios. Isso acontece, porque o trabalho real e os exercícios são feitos de modo simultâneo e contínuo, mas o trabalho real se sobrepõe a qualquer dos exercícios, já que a falha nele, pode trazer impactos imediatos.

A rede de exercícios visa imitar um ataque real à organização. Quando preparada pelo *cyber purple team*, o *cyber red team* será responsável por realizar esse ataque. Esses ataques foram testados anteriormente e, portanto, devem ser eficazes. O papel do *cyber blue team* é ser capaz de identificar e corrigir a falha na rede de exercícios o mais rápido possível. Nessa rede de exercícios, o *cyber purple team* é o responsável por controlar o exercício e as equipes, e pode até determinar pontos de partida para o ataque. Essa ação dependerá da necessidade de avaliar as defesas em profundidade e todas as etapas da implementação.

Na rede de exercícios, o *cyber red team* deve tentar ofuscar os ataques para que o *cyber blue team* não possa identificar. O final do exercício pode ser obtido a partir do cumprimento do objetivo imposto ao *cyber red team* ou o a completa anulação do ataque, feita pelo *cyber blue team*. Para acontecer a anulação deve-se também garantir que a falha explorada foi corrigida e, não permite mais que o mesmo ataque seja replicado.

Diversas parâmetros podem ser determinados pelo *cyber purple team* para controle das atividades, um que foi utilizado fixamente na metodologia foi o tempo. Essa métrica que pode ser aplicada na rede experimental e na de exercício. Na rede experimental, caso o ataque não for desenvolvido dentro do prazo estabelecido, o *cyber purple team* deve alterar a perspectiva do ataque ou alterar a rede alvo.

A métrica de tempo é determinada porque se não for possível várias redes de exercícios e experimentos em paralelo, a atividade pode ficar travada por muito tempo se não houver a conclusão do trabalho pela equipe responsável. A mesma métrica de tempo é aplicada na rede de execícios para que ele não dure um tempo além do previsto, mas no caso do tempo se esgotar na rede de exercícios, dá-se o *cyber blue team* como equipe vitoriosa do confronto, pois conseguiu se resguardar.

O *cyber purple team* também deve ser responsável por medir os resultados obtidos em todas as redes da metodologia. Sendo assim, deve-se ter a capacidade de coletar dados sobre aspectos do exercício, como: Efetividade do Ataque (EA), Tempo de Identificação do Ataque (TIA), Tempo de Ocultação do Ataque (TOA), Tempo de Cálculo de Danos (TCD).

O *cyber purple team* também deve colher todos os dados para que seja possível gerar estatísticas de acompanhamento, e assim acompanhar a evolução das equipes. Pois futuramente, essas estatísticas devem ser apresentadas ao alto comando da organização militar para o conhecimento e avaliação do desempenho e também devem ser usadas durante o exercícios para controle.

A partir desses conhecimentos gerados pelas estatísticas, poderão ser direcionados novos exer-

cícios, para aquisição de novas habilidades, as quais o alto comando julgue necessárias. O *cyber purple team* poderá gerar diversas métricas, conforme as necessidades de avaliação de desempenho, por isso, o *cyber purple team* deve ter as habilidades necessárias para entregar informações de valor às equipes e também à alta gestão da organização militar.

4.3.4 4º passo: Homologar as correções feitas

Após a conclusão de um exercício, o *cyber blue team* deve fazer as alterações necessárias na rede de exercícios, para evitar ou ameninar o ataque cibernético do exercício. Com isso, a metodologia irá cumprir seu fim, que é permitir que os ataques sejam corrigidos antes de serem explorados por agentes reais e também imputar no *cyber red team* a habilidade de explorar a mesma falha.

Após a correção da falha explorada na rede de exercícios pelo *cyber red team*, essa correção já será validada em tempo real dentro do próprio exercício e então poderá ser implementada na rede produção, tendo passado por testes.

4.3.5 5º passo: Gerar estatística final e corrigir as falhas na rede de produção

Depois de ocorrido o ataque, caso o *cyber blue team* não tiver conseguido identificá-lo dentro do prazo estabelecido, o *cyber red team* deverá enviar ao *cyber blue team* um relatório sobre as ações realizadas. Este relatório é enviado por meio do *cyber purple team* e deve detalhar tudo o que foi feito no ataque, e com base nesse relatório, o *cyber blue team* deve implementar correções na rede de produção. Esse atalho existe para que a organização não fique vulnerável por muito tempo.

Com o relatório feito pelo *cyber red team* em mãos ou baseados nas correções implementadas na rede de exercícios, o *cyber blue team* , nesse passo, deve colocar as correções no ambiente de produção. Com isso finaliza-se um rodada da metodologia, na qual cumpre-se o objetivo de treinar o ataque e a defesa.

Enquanto isso, o *cyber purple team* deve ser capaz de gerar a informação baseada em todas as métricas definidas. Os dados devem ser capturados ao decorrer de todas as fases. Abaixo, segue uma lista de todos os dados que devem as métricas que devem ser capturadas, no entanto, podem existir variações, já que depende das necessidades específicas de cada organização militar.

- Tempo de Desenvolvimento de Ataques (TDA)
- Efetividade do Ataque (EA)
- Tempo de Identificação do Ataque (TIA)
- Tempo de Ocultação do Ataque (TOA)
- Tempo de Cálculo de Danos (TCD)

- Tempo de Implementação da Defesa (TID)
- Tempo Total para Defesa (TTD)

Já com todas as correções efetuadas e o ataques feitos pelo *cyber red team* não for mais possível de ser replicado em rede de produção, o fluxo da metodologia deverá ser reiniciado. A rede de produção deve ser selecionada e clonada novamente em uma rede experimental. Logo após, uma rede de exercícios com as características já descritas também deve ser criada, reiniciando o ciclo. O ciclo da metodologia de treinamento contínuo é ilustrado na Figura 4.5.

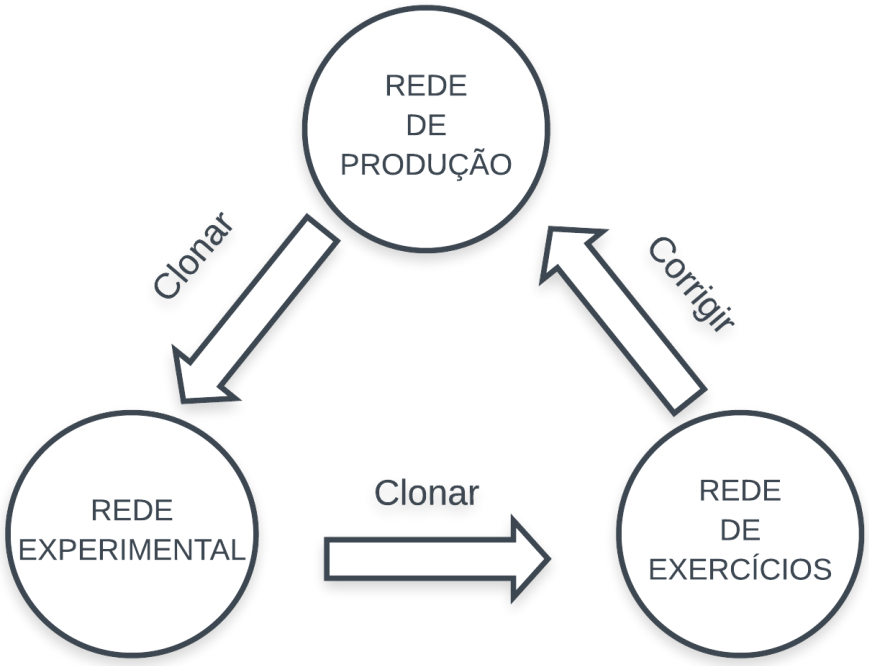

Figura 4.5: Ciclo de vida da metodologia proposta.

4.4 LABORATÓRIO

Utilizando-se desse laboratório, foi possível comprovar a necessidade de se ter habilidades específicas dentro dos *cyber teams* militares e a eficácia da metodologia proposta. Essa experiência contou com a participação de dezessete militares. Desses militares, dez formaram o *cyber blue team* , cinco o *cyber red team* e dois o *cyber purple team*. Os militares participaram integralmente dos exercícios, pois ele era aberto a toda a equipe, sem prejuízo ao trabalho real. Esse experimento se estendeu por um período de 9 meses aproximadamente.

4.4.1 Infraestrutura do laboratório

O laboratório foi desenvolvido com base em uma estrutura que foi copiada integralmente das redes de produção da organização militar, onde foram demandados os testes. Essa infraestrutura

copiada obedeceu integralmente o que foi proposto dentro da metodologia. A Figura 4.6 representa a arquitetura mantida em todas as rodadas na rede experimental, onde o *cyber red team* desenvolve os ataques cibernéticos. A parte retangular azul, representa todos os ativos presentes dentro da rede alvo. O círculo pontilhado representa ativos que podem ou não estar presentes. Essa variação depende das peculiaridades da rede que será testada.

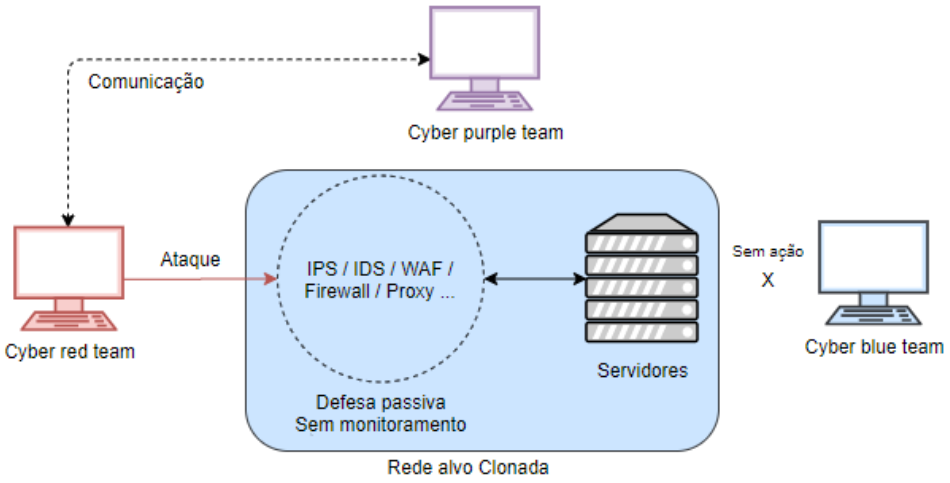

Figura 4.6: Infraestrutura da rede experimental no laboratório

Como pode ser percebido na Figura 4.6, não existe ação e monitoramento do *cyber blue team*, no entanto, as defesas já implementadas permanecem ativas dentro da rede. Esse é o fato que torna o desenvolvimento dos ataques cada vez mais desafiador para o cyber red team, pois ao decorrer das rodadas de teste, as defesas pré-estabelecidas tendem apenas a aumentar.

Já a Figura 4.7 representa a rede de exercícios. Nessa rede podemos notar ação total de todas as equipes, da mesma forma como previsto na metodologia proposta. Ela é muito semelhante a rede experimental, no entanto, conta com o monitoramento ativo do *cyber blue team* e sua interferência imediata em casos de ataque.

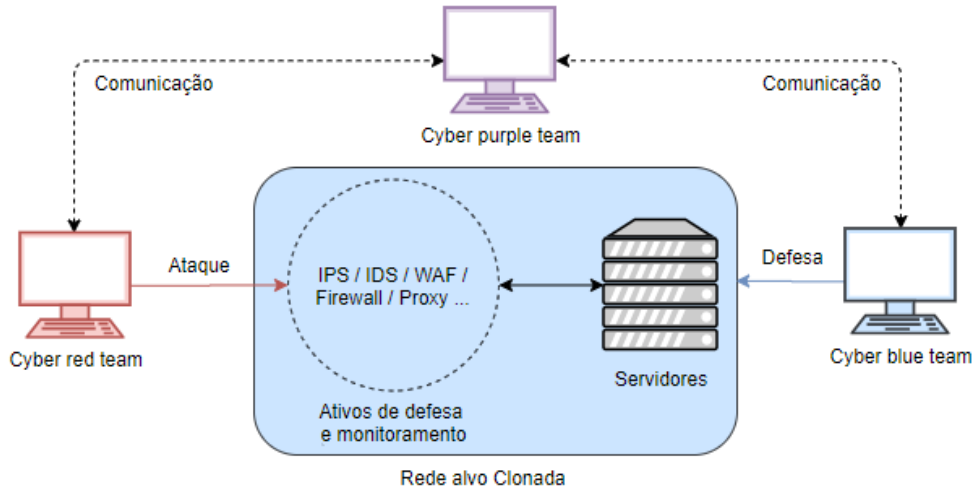

Figura 4.7: Infraestrutura da rede de exercícios no laboratório

A terceira rede é a rede de produção. Essa rede não está dentro do escopo do laboratório, ela serve apenas como base para os exercícios e é de inteira responsabilidade do *cyber blue team*. Não incide nela, qualquer ação de outras equipes.

Tanto na Figura 4.2 quanto na 4.7 existem canais para comunicação com o *cyber purple team*. Com base nessa comunicação podem ser feitos ajustes nas redes e também captura de dados, aos quais serão utilizados para gerar estatística futuramente.

4.4.2 Coleta de dados dentro do experimento

A coleta de dados para este trabalho foi baseada nas necessidades de uma organização militar. A Tabela 4.2 exibe os dados coletados pelo *cyber purple team* durante todo o período do laboratório, de acordo com os parâmetros exigidos pela metodologia proposta. Esses dados foram adquiridos como os *feedbacks* repassados por cada equipe. Isso aconteceu por meio de um canal de comunicação que fica fora do escopo dos exercícios da metodologia.

Durante o experimento foi possível realizar quinze rodadas de exercícios de confronto. Essas rodadas foram separadas em cinco grupos, cada grupo contém um ataque a confidencialidade (C), um ataque contra a integridade (I) e outro contra a Disponibilidade (D). Esses ataques são classificados de acordo com os princípios da segurança da informação [42]. Essa escolha foi feita para que todos os princípios sejam alvo de ataque, no entanto, essa necessidade pode variar de acordo com os objetivos de cada organização militar.

O TDA (Tempo de Desenvolvimento de Ataques) é um parâmetro que mede quanto tempo levou para desenvolver cada ataque dentro da rede experimental, em horas. A métrica EA (Efetividade do Ataque) é anotada com "S", caso o ataque desenvolvido pelo *cyber red team* resultou no cumprimento total do objetivo imposto. Se o objetivo foi parcialmente atingido é atribuindo a letra "P"e a falha em alcançar o objetivo é "N".

Os parâmetros TIA (Tempo de Identificação do Ataque), TCD (Tempo de Cálculo de Danos) e TID (Tempo de Implementação da Defesa) compõe o TTD (Tempo Total para Defesa). A métrica TIA mede a eficácia do *cyber blue team*. O TOA (Tempo de Ocultação do Ataque) é o mesmo valor do parâmetro TIA que serve para avaliar o *cyber red team*, porque quanto mais tempo o *cyber blue team* leva para identificar o ataque cibernético, mais eficaz é a ofuscação dos ataques realizados. A diferença entre TIA e TOA, é o ponto de vista. O TIA se aplica à efetividade do *cyber blue team* e o TOA ao *cyber red team*.

Em todas as fases da metodologia até esse momento, o *cyber purple team* foi capaz de coletar os dados mostrados na Tabela 4.2, por meio de comunicação com as equipes participantes. Todos os valores numéricos são de tempo e são expressos em horas, tabela está separada em grupos e cada um desses grupos contém um ataque a cada princípio do CID[42]. A tabela 4.2 também especifica as rodadas que somam o total de quinze, separadas em 5 grupos.

Tabela 4.2: Dados coletados no experimento

Grupo	**A**			**B**			**C**			**D**			**E**		
Rodada	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
Objetivo	C	I	D	I	D	C	D	I	C	C	D	I	I	D	C
TDA	02	03	01	10	06	15	12	45	30	28	80	54	103	44	88
EA	P	S	N	S	S	S	P	S	S	N	S	S	P	N	S
TIA/TOA	02	120	05	15	04	26	14	30	93	32	120	19	24	03	76
TCD	15	120	01	23	01	20	04	16	50	12	120	72	18	01	15
TID	10	01	02	04	01	30	01	06	01	04	02	24	14	03	12

Legenda

C: Confidencialidade; **D**: Disponibilidade; **EA**: Efetividade do Ataque; **I**: Integridade; **N**: Não; **P**: Parcial; **S**: Sim. **TCD**: Tempo de Cálculo de Danos; **TDA**: Tempo de Desenvolvimento de Ataques; **TIA**: Tempo de Identificação do Ataque; **TID**: Tempo de Implementação da Defesa; **TOA**: Tempo de Ocultação do Ataque; **TTD**: Tempo Total para Defesa;

4.5 ATAQUES DESENVOLVIDOS DURANTE O LABORATÓRIO

Durante o laboratório foram desenvolvidos diversos ataques pela equipe do *cyber red team*, no entanto, como não se trata de apenas um *pentest* esses ataques foram combinados nos exercícios, em prol de um objetivo estabelecido previamente. Entre esses ataques desenvolvidos podemos citar ataques de injeção de comandos no banco de dados e no sistema operacional, ataques de inclusão de arquivos maliciosos nos servidores, exploração de aspectos permitidos por má configuração dos servidores, exploração de serviços em versão vulnerável, etc.

Além dos ataques que levaram em consideração as habilidades técnicas de cibernética, também utilizou-se de ataques de engenharia social para realizar os objetivos. A combinação entre engenharia social e ataques cibernéticos foram de grande efetividade e resultaram em grandes vantagens para o *cyber red team* ao decorrer das atividades. Além disso, aspectos relativos a segurança física também entram em cena.

O detalhamento de cada ataque, não pode ser exibido neste trabalho, pois se trata de sistemas reais que foram levados a prova nessas simulações. Como se trata de informações sensíveis de Estado, alguns dados tiveram que sofrer sanitização. Sua divulgação de forma ampla e pública poderiam acarretar em ataques cibernéticos com sucesso. Devido a isso, optou-se por mantê-las em sigilo, para que durante a aplicação da metodologia de treinamento contínuo proposta haja a correção das vulnerabilidades.

4.6 ANÁLISE DOS RESULTADOS OBTIDOS

Uma variedade de informações pode ser extraída da Tabela 4.2. Com isso, pode-se transformá-la em informações que agregam valor as equipes e informem ao alto comando as necessidades e o nível que as equipes se encontram. Nos tópicos a seguir, seguem diversas informações e análises que puderam ser extraídas dos dados estatísticos capturados no laboratório.

4.6.1 Tempo de desenvolvimento dos ataques

O gráfico mostrado na Figura 4.8 mostra, claramente, a evolução dos ataques cibernéticos na rede experimental. O gráfico é dividido pela evolução dos ataques cibernéticos que afetam cada princípio da CID (Confidencialidade, Integridade e Disponibilidade).

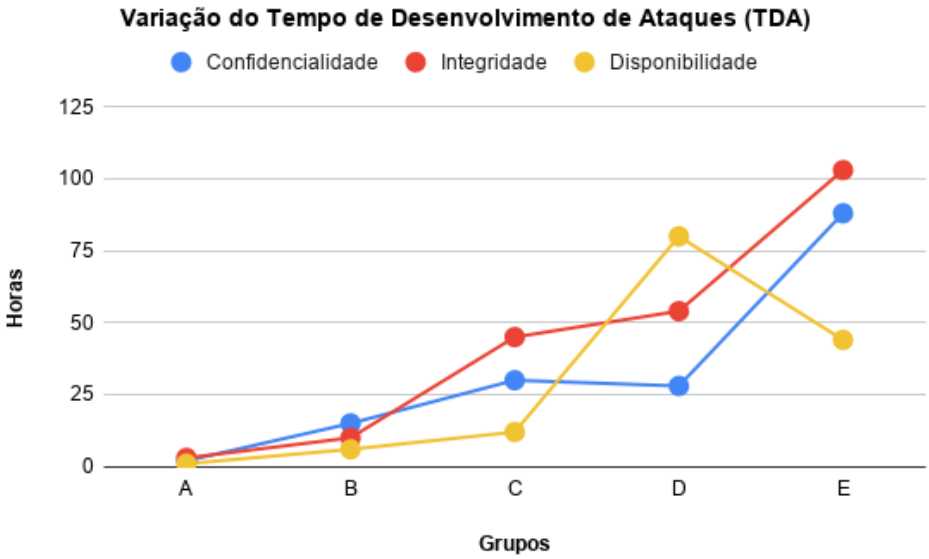

Figura 4.8: Gráfico do tempo de desenvolvimento dos ataques.

No gráfico mostrado na Figura 4.8, pode-se notar que há um aumento progressivo na métrica TDA. Percebe-se que há uma ligeira queda nos ataques que afetam a confidencialidade dos exercícios do grupo D e uma queda mais significativa nos ataques a disponibilidade no grupo E. Essas diminuições de tempo de desenvolvimento podem acontecer sempre e de forma repentina, a depender das vulnerabilidades que são divulgadas e até mesmo na produção dos *exploits* externos, que já entregam para o *cyber red team* uma arma pronta em alguns casos.

O aumento no tempo de desenvolvimento dos ataques é natural e deve-se ao fato de que a cada ataque realizado, o *cyber blue team* implementava defesas eficazes. Essas defesas são colocadas em produção e podem ser reaproveitadas em outras redes e sistemas. Então, essas ações exigem cada vez mais tempo para o desenvolvimento de novos ataques, já que quanto maior o nível de defesas implementadas, maior a dificuldade para o *cyber red team*. Essa dificuldade requer, do

cyber red team, o aprendizado de novas técnicas de ataque para transpassar as novas defesas implementadas. O gráfico 4.8 mostra, claramente, que as defesas melhoram à medida que novas técnicas e conhecimentos sobre ataques são adquiridos e executados pelo *cyber red team*.

4.6.2 Efetividade dos ataques

Logo após o desenvolvimento dos ataques pelo *cyber red team*, eles foram executados na rede de exercícios, onde o *cyber blue team* tem monitoramento. O gráfico na Figura 4.9 exibe a porcentagem relativa à efetividade desses ataques desenvolvidos na rede experimental, quando aplicados na rede de exercícios contra o *cyber blue team*.

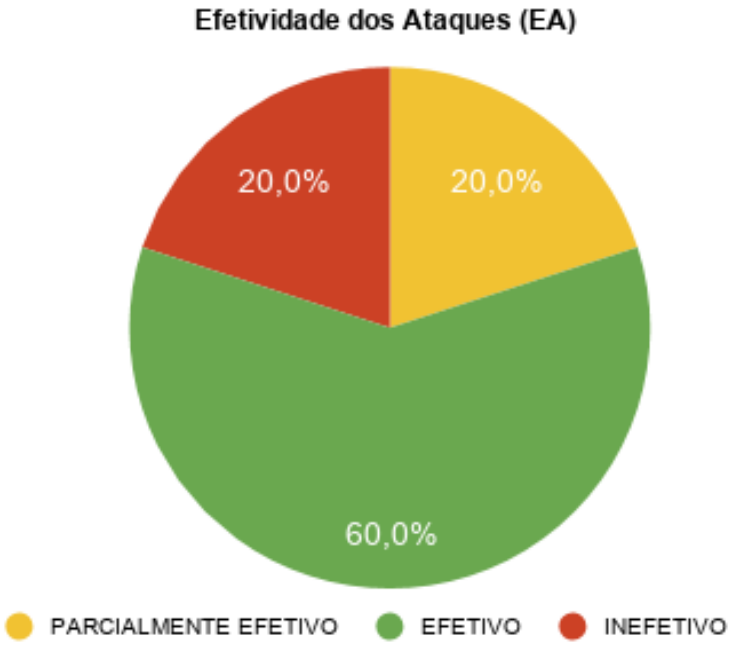

Figura 4.9: Gráfico da efetividade dos ataques.

No gráfico da figura 4.9, dos quinze ataques realizados na rede de exercícios, vinte por cento não foram efetivos, ou seja, o *cyber blue team* se preparou de forma a evitar esses ataques. Quando o *cyber blue team* pode identificar e bloquear o ataque antes que o objetivo seja atingido pelo *cyber red team*, pode-se ter duas outras possibilidades. O objetivo pode ser "NÃO", onde não houve perda pela equipe de defesa ou "PARCIAL", onde existiu uma perda relativa, menor que o máximo que poderia acontecer se o ataque ocorresse perfeitamente.

4.6.3 Tempo de identificação e ofuscação dos ataques

Com relação à eficiência do ataque e da defesa, temos duas métricas que são o TOA e o TIA. Quando essas métricas são aplicadas às diferentes equipes, são parâmetros inversamente proporcionais. Se o TIA é alto, significa que o *cyber red team* está se escondendo por mais tempo

e, se é baixo, significa que o *cyber blue team* está identificando mais rapidamente o ataque. O TOA representa o contrário, porque mede o *cyber red team* e é o mesmo valor de forma inversa. O gráfico da Figura 4.10 mostra a evolução desse parâmetro nas perspectivas de ambas as equipes.

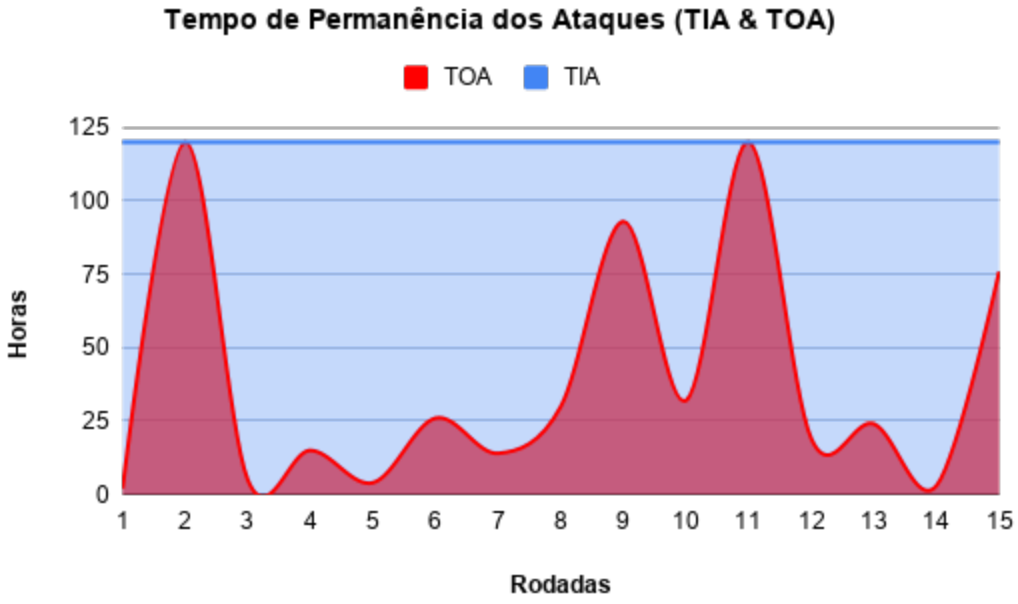

Figura 4.10: Gráfico do tempo de identificação e ofuscação dos ataques.

O gráfico na Figura 4.10 mostra uma disputa entre o *cyber blue team* e o *cyber red team*. Quanto maior a curvatura vermelha, mais tempo durou ataque. No caso dos exercícios número dois e onze, o ataque excedeu o limite de tempo estabelecido pelo *cyber purple team* para todo o exercício, que como limite, definiu o prazo de cento e vinte horas.

4.6.4 Tempo de cálculo dos danos

As métricas relativas ao *cyber blue team* também são analisadas. O *cyber blue team* deve ser capaz de quantificar os danos de forma rápida e precisa, para que as medidas possam ser tomadas de forma mais eficiente. Com o conhecimento dos danos, o *cyber blue team* pode realizar as suas ações reparativas em pontos específicos, por exemplo, ao saber que senha de cem usuários foram vazadas, pode-se obrigar de forma instantânea os mesmos a trocarem suas senhas, ou até mesmo, realizar um esforço maior de monitoramento em cima dos alvos mais prováveis. A Figura 4.11 exibe a evolução no tempo de cálculo de danos feito pelo *cyber blue team*, separados pelas rodadas de exercícios.

Ao analisar a Figura 4.11, nota-se uma variação na linha, o que indica que ao decorrer das rodadas de exercícios o tempo de cálculo de danos variou entre valores altos e baixos. Essas curvas indicam a evolução constante do *cyber blue team* e do *cyber red team*, pois da mesma forma que o *cyber blue team* adquire novas capacidades de realizar os cálculos de forma mais precisas, o *cyber red team* também adquire as habilidades que dificultam a descoberta de suas

ações, o que impacta diretamente no tempo para o cálculo dos danos.

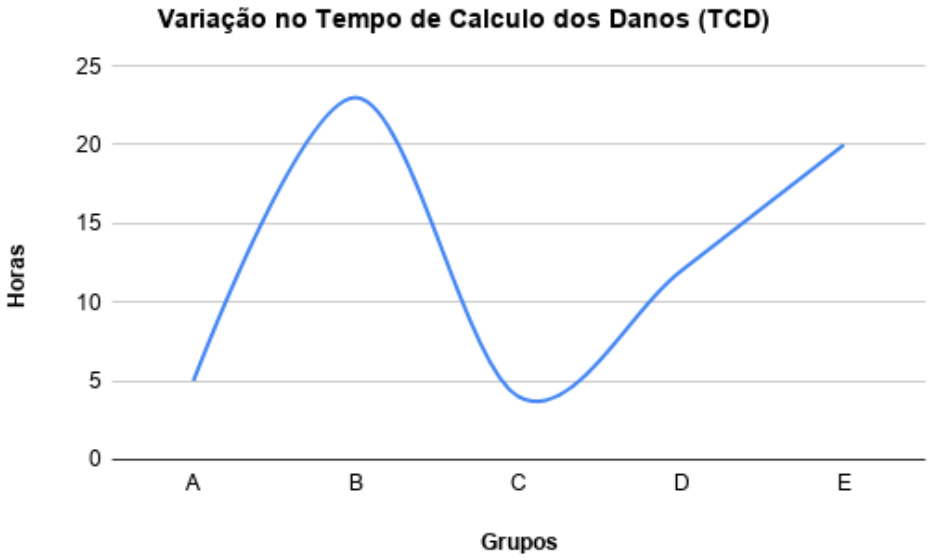

Figura 4.11: Gráfico do tempo de cálculo dos danos

4.6.5 Tempo para implementação das defesas

Para além do tempo de cálculo de danos, existe o tempo que o *cyber blue team* levou para mitigar totalmente a vulnerabilidade da infraestrutura. Esse dado é importante que seja o mais rápido possível, pois a existência de uma vulnerabilidade por muito tempo, abre espaço para ataques reais na infraestrutura. A Figura 4.12 exibe a evolução do *cyber blue team* nesse quesito.

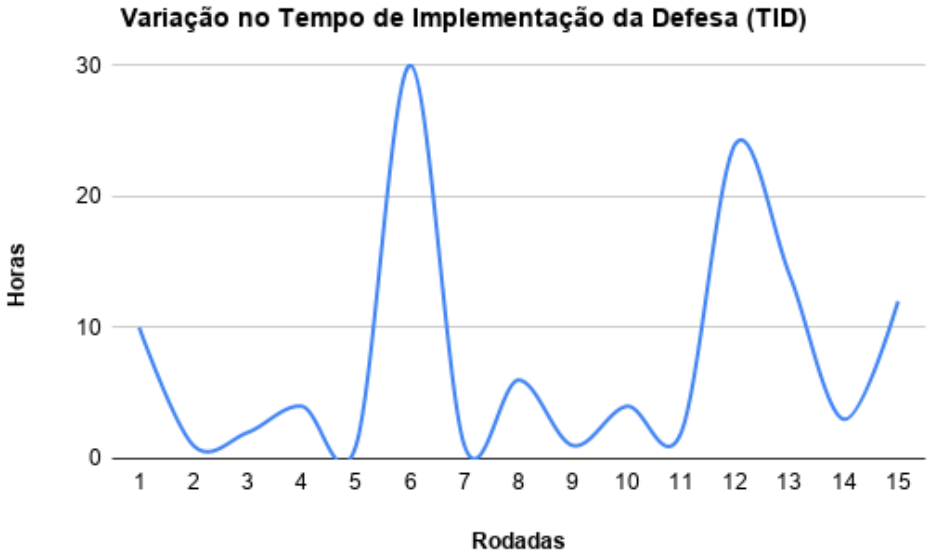

Figura 4.12: Gráfico do tempo para implementação das defesas.

Com o gráfico apresentado na Figura 4.12, nota-se dois picos no tempo de implementação das defesas, apesar que de um modo geral o gráfico se mantém com valores baixos, o que é favorável. Os picos são normais para alguns tipos de vulnerabilidades que exigem correções complexas, por vezes o fabricante do software ainda não desenvolveu *patchs* para a correção da vulnerabilidade, o que obriga o *cyber blue team* a desenvolver uma solução preventiva, o que faz o processo de mitigação levar mais tempo para ser concluído.

4.6.6 Tempo total de tratamento do incidente

O gráfico na Figura 4.13 mostra o tempo total, em horas para o tratamento e implantação de defesas. Este índice caracteriza a evolução do *cyber blue team* e relação ao aspecto total da defesa. A métrica TTD representa realmente o tempo total para o *cyber blue team* restabelecer a condição de não vulnerável, onde todos os tratamentos, cálculos de prejuízo e correções já foram executados.

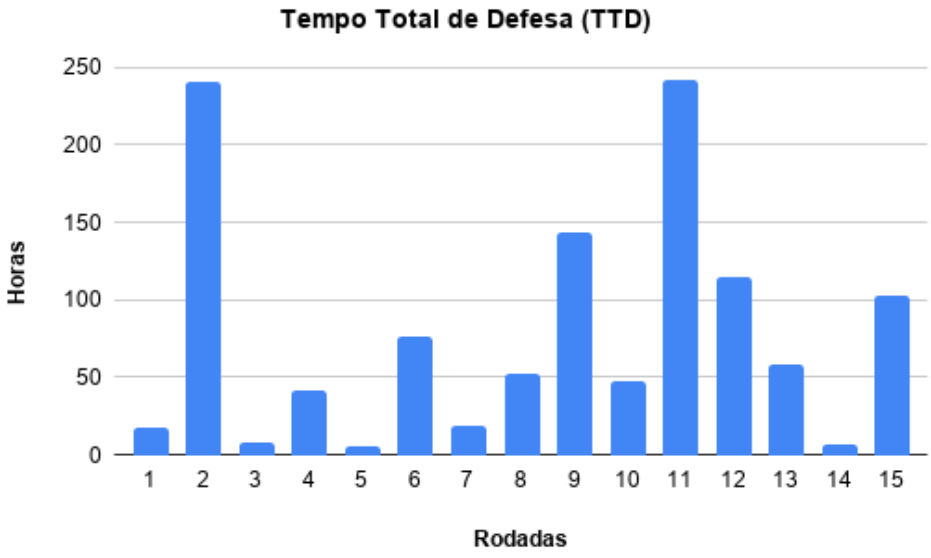

Figura 4.13: Gráfico do tempo total de tratamento do incidente.

O gráfico da Figura 4.13 mostra uma certa alternância no tempo total de desenvolvimento, que caracteriza o crescimento em conjunto com o *cyber red team*, o qual é o objetivo dessa metodologia. A variação, caracteriza o ganho múltiplo de habilidades pelas duas equipes. Esse gráfico tende a possuir cada vez menos variações em percentuais, devido ao crescimento das equipes.

4.6.7 Análise geral

Todos os gráficos apresentados neste experimento mostram claramente a melhoria contínua do *cyber blue team* e o *cyber red team*. Evidenciando que ambas as equipes adquiriram novas

habilidades e também melhoraram suas eficiências. Como a eficiência do ataque e da defesa são inversamente proporcionais, para que exista uma evolução das das equipes de uma forma simultânea, a linha de medição no gráfico deve sempre variar em senoide. O alto nível de habilidades das equipes podem ser medidas de acordo com o nível dessa variação, quanto menor a variação, mas eficazes estão as equipes, no entanto, a variação zero não pode ocorrer, pois nesse caso não aconteceria sucesso em ataques do *cyber red team* e caso ocorresse o problema deve ser identificado e corrigido pelo *cyber purple team*.

5 CONCLUSÃO

No contexto militar existem diversas peculiaridades, que são incomuns aos outros tipos de organizações. Mediante isso, torna-se mais complexa a montagem de um *cyber red team* nesse contexto. É preciso abranger uma vasta gama de competências não exigidas em outros tipos de organizações.

Como o ambiente militar exige uma multidisciplinaridade grande, devido a vasta amplidão de competências que envolve uma guerra, essa exigência acaba também sendo transferida para as competências necessárias às equipes cibernéticas. Tanto a equipe de defesa como a de ataque deve possuir competências em todas essas áreas para que o trabalho dentro da cibernética seja efetivo.

A partir do estudo feito nesta dissertação, chegou-se a conclusão que existem quatro competências macro para os *cyber red teams*, as quais devem ser totalmente atendidas. Com base nessas competências, foram identificadas outras quatro, originadas por meio de suas intersecções em conjunto com as peculiaridades de um ambiente operacional militar. Essas, por sua vez, já trazem consigo características que abrangem o ambiente militar com suas peculiaridades. No entanto, ainda não trazem o refino necessário para que a efetividade de um *cyber red team* militar seja aumentada.

Na busca por um refinamento mais aprofundado, foram identificadas mais quatro competências de alto valor para o ambiente militar, todas elas originadas a partir de intersecções sucessivas com todas as anteriores. Essas últimas quatro competências identificadas são as mais próximas das ações de um *cyber red team* militar e finalizam o estudo de identificação das competências inerentes a este contexto. Com base no estudo feito neste trabalho, é proposto um diagrama de competências que leva em consideração as peculiaridades no contexto militar e apresenta de forma sucinta e visual todas as competências necessárias, para formulação de um *cyber red team* nesse contexto.

Com as competências para os *cyber red teams* definidas, é necessário montar um processo de seleção desses profissionais, que está fora do escopo dessa dissertação, pois depende das peculiaridades de cada Estado. Já com o processo de seleção feito e todos os profissionais à disposição, torna-se necessário que, o *cyber red team* continue a ampliar suas habilidades. Para isso é necessário que exista uma interação com a equipe de defesa, de modo que seja possível um aprendizado mútuo.

Diante dessa necessidade, esta dissertação propõe, de modo a complementar a atividade, uma metodologia de treinamento contínuo que não exige que os profissionais se envolvam exclusivamente nos exercícios, o que faz com que o trabalho real não seja deixado de lado e o treinamento também se perpetue. Dessa forma permite-se uma evolução contínua das habilidades cibernéticas sem impacto no trabalho. Como resultado dos experimentos realizados, observou-se que as ha-

bilidades para defesa cibernética, reconhecimento e ataque, pré-requisitos para projetar o poder militar na guerra cibernética, aumentaram continuamente ao longo do experimento.

Durante a dissertação foram coletados dados nos laboratórios desenvolvidos como experimento, neles foram constatados uma tendência de melhora nas habilidades de defesa e de ataque. Esses dados foram capturados pelo *cyber purple team*, equipe gerenciadora da metodologia e responsável pela estatística, que poderão ser futuramente apresentadas aos altos comandos das forças armadas que implementarem a metodologia.

Os dados coletados pelo *cyber purple team* através do uso da metodologia proposta também podem melhorar as regras de detecção de ataques e ainda encontrar falhas no processo de implementação de defesa e tratamento de incidentes. Tudo isso depende da demanda pelas estatísticas. No caso do laboratório executado na dissertação, restringiu-se ao escopo de mostrar apenas a eficiência da metodologia proposta.

Por fim, pode-se concluir que o trabalho proposto que abrange desde os estabelecimentos dos requisitos para se ter um *cyber red team*, até a aplicação de uma metodologia de treinamento contínuo eficiente. Os dados coletados pelo laboratório exibe que, seguindo as diretrizes do trabalho, tem-se um incremento contínuo das habilidades das equipes ofensivas e defensivas e também na gestão pelo *cyber purple team*, onde são gerados métricas para o alto comando. Com isso, afirma-se que a metodologia proposta é altamente funcional e contribui totalmente para os itens necessários para projetar o poder militar em meio a uma guerra cibernética, pois fortalece firmemente todos os requisitos necessários para um guerra neste meio.

5.1 TRABALHOS FUTUROS

A dissertação apresentada pode ter sua eficiência ainda mais incrementada a partir do desenvolvimento de tecnologias e metodologias que a complementem. Esses aspectos a serem desenvolvidos, além de colaborar para o público alvo dessa dissertação, que é apenas as equipes cibernéticas militares, também auxiliária todo o efetivo militar. Isso consequentemente aumentaria ainda mais o poder cibernético. Abaixo segue alguns itens a serem incrementados, que colaborariam para um maior ganho de habilidades por partes das equipes e todo o corpo militar.

5.1.1 Metodologia de seleção e recrutamento de profissionais

Sabe-se que a contratação de profissionais de segurança da informação não é algo fácil. Muitos desses profissionais são de comportamento inapropriados para um emprego convencional e preferem estar mais presentes no mundo anônimo do que projetar suas carreiras em empresas ou órgãos do governo pelo mundo a fora. Essa peculiaridade pode trazer grandes dificuldades para diversas organizações que necessitam desse tipo de serviço.

Devido a isso, é completamente necessário um estudo que seja capaz de imergir neste meio de

profissionais e trazer a tona motivações para que aconteça seu recrutamento e seleção. As forças armadas dos países teriam seus poderes altamente ampliados, por meio da participação desses profissionais em suas equipes.

5.1.2 Software inteligente de produção de tráfego de rede

Na rede de exercícios não existe interação de pessoas que sejam além das equipes pré-definidas e nem de clientes dos serviços em comum. Essa peculiaridade, traz para o *cyber blue team* uma certa facilidade na identificação, pois toda ação feita, na rede de exercícios, pode ser considerada suspeita. Isso delega para o *cyber red team* uma dificuldade adicional, pois tem de simular tráfego de rede extra para tentar ofuscar as suas ações.

Os benefícios de um software como esse seria, que o *cyber red team* irá poder adquirir capacidades de encontrar um momento ideal para certo tipo de ataque. Essa ação dificultaria o trabalho *cyber blue team*, que também seria treinado na mesma proporção. Esse software serviria, como potencializador de toda a metodologia e deveria ser configurado pelo *cyber purple team*, de acordo as habilidades necessárias no momento. Como seria inclusive possível, programar outros ataque automáticos para amplificar a capacidade de priorização do *cyber blue team*.

5.1.3 Metodologia para manobra militar cibernética

A metodologia desenvolvida nesta dissertação teve o seu foco nas equipes cibernéticas das forças armadas. No entanto, entende-se a necessidade de expansão dessa metodologia a todo efetivo. Uma operação militar focada neste tipo de ação, trará um consciência grande do poder relacionado a cibernéticas para todos os componentes. Com isso, todos estariam mais preparados para lidar com possíveis ataques cibernéticos.

Referências Bibliográficas

1 Parks, R. C.; Duggan, D. P. Principles of cyberwarfare. *IEEE Security Privacy*, v. 9, n. 5, p. 30–35, Sep. 2011. ISSN 1540-7993. ISSN: 1540-7993.

2 Dandurand, L. Rationale and blueprint for a cyber red team within nato: An essential component of the alliance's cyber forces. In: *2011 3rd International Conference on Cyber Conflict*. [S.l.: s.n.], 2011. p. 1–16. ISSN 2325-5366. Tallinn, Estonia. ISSN 2325-5366.

3 JUNIOR, J. A. de A.; GIOZZA, W. F.; ALBUQUERQUE, R. d. O.; NZE, G. D. A.; CANEDO, E. D.; FILHO, D. A. d. S. Competências para os cyber red teams no contexto militar. *RISTI*, v. 26, p. 612–623, 2020.

4 BARRETT, E. T. Warfare in a new domain: The ethics of military cyber-operations. *Journal of Military Ethics*, Taylor & Francis, v. 12, n. 1, p. 4–17, 2013.

5 ZENKO, M. *Red Team: How to succeed by thinking like the enemy*. 250 West 57th Street, New York, NY 10107: Basic Books, 2015. ISBN 978-0-465-07395-5.

6 MANSFIELD-DEVINE, S. The best form of defence – the benefits of red teaming. *Computer Fraud Security*, v. 2018, n. 10, p. 8 – 12, 2018. ISSN 1361-3723. ISSN: 1361-3723. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1361372318300976>.

7 LINDSAY, J. R. Stuxnet and the limits of cyber warfare. *Security Studies*, Taylor & Francis, v. 22, n. 3, p. 365–404, 2013.

8 PTES. *Penetration Testing Execution Standard*. 2009. URL: http://www.pentest-standard.org/index.php/ PTES_Technical_Guidelines. Access in 01 jun 2019 19:36.

9 SHARMA. *Hands-on red team tactics: A practical guide to mastering Red Team operations*. Livery Place, 35 Livery Street, Birmingham B3 2PB, UK.: Packt Publishing Limited, 2018. ISBN 978-1-78899-523-8.

10 CYLANCE, B. Report: Thin red line - penetration testing practices examined. *ThreatVector*, 2019. URL: https://threatvector.cylance.com/en_us/home/report-thin-red-line-penetration-testing-practices-examined.html.

11 BRANGETTO, P.; CALISKAN, E.; ROIGAS, H. Cyber red teaming-organisational, technical and legal implications in a military context. *NATO CCD CoE*, 2015. Filtri tee 12, Tallinn 10132, Estonia. URL: https://ccdcoe.org/uploads/2018/10/Cyber_Red_Team.pdf.

12 GÓMEZ, M. O. Procurando um modelo de resiliência cibernética baseado nas experiências da otan e sua possível transferência para américa do sul. 2019.

13 DAWSON, J.; THOMSON, R. The future cybersecurity workforce: going beyond technical skills for successful cyber performance. *Frontiers in psychology*, Frontiers Media SA, v. 9, 2018.

14 ARMY, U. Cyberspace operations concept capability plan 2016-2028. *US Army Capabilities Integration Center*, v. 22, 2010.

15 DEFESA, M. Doutrina militar da defesa cibernética. *D.O.U. nº 224*, nov 2014. Portaria normativa nº 3.010/MD. URL: https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf.

16 JÚNIOR, D. P.; DUARTE, É. E. Projeção de poder e intervenção militar pelos estados unidos da américa. *Revista Brasileira de Política Internacional*, SciELO Brasil, v. 46, n. 1, p. 135–152, 2003.

17 REGAN, R. Red teaming: Why a forward offense is the best defense. *SECURE Magazine*, 2019. URL: URL: https://www.helpnetsecurity.com/2019/08/19/red-teaming/.

18 ICITS, I. Disponível em:<http://www.icits.me/index.php/>. *Acessado em 21/04/2020 as 18:19*, v. 0, 2019.

19 AISTI, R. Disponível em:<http://www.risti.xyz/>. *Acessado em 21/04/2020 as 17:34*, v. 0, 2008.

20 Chen, Z.; Yan, L.; He, Y.; Bai, D.; Liu, X.; Li, L. Reflections on the construction of cyber security range in power information system. In: *2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*. [S.l.: s.n.], 2018. p. 2093–2097. ISSN 2381-0947.

21 FANG, B.; JIA, Y.; LI, A.; ZHANG, W. Cyber ranges: state-of-the-art and research challenges. *Journal of Cyber Security*, v. 1, n. 3, p. 1–9, 2016.

22 CARR, J. *Inside cyber warfare: Mapping the cyber underworld*. [S.l.]: " O'Reilly Media, Inc.", 2011.

23 SCHMITT, M. N. *Tallinn manual on the international law applicable to cyber warfare*. [S.l.]: Cambridge University Press, 2013.

24 Eom, J.; Kim, N.; Kim, S.; Chung, T. Cyber military strategy for cyberspace superiority in cyber warfare. In: *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*. [S.l.: s.n.], 2012. p. 295–299. Kuala Lumpur, Malaysia. DOI 10.1109/CyberSec.2012.6246114.

25 BUCHLER, N.; FLEUR, C. G. L.; HOFFMAN, B.; RAJIVAN, P.; MARUSICH, L.; LIGHTNER, L. Cyber teaming and role specialization in a cyber security defense competition. *Frontiers in psychology*, Frontiers Media SA, v. 9, 2018.

26 DIOGENES, Y.; OZKAYA, E. Cybersecurity, attack and defense strategies: infrastructure security with red team and blue team tactics. Packt Publishing, 2018.

27 YAMIN, M. M.; KATT, B.; GKIOULOS, V. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers Security*, v. 88, p. 101636, 2019. ISSN 0167-4048. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0167404819301804>.

28 CHIAVENATO, I. *Introdução à teoria geral da administração*. [S.l.]: Elsevier Brasil, 2003.

29 WEINBERG, G. M. *Becoming a technical leader*. [S.l.]: Dorset House Publishing Company, Incorporated, 1986.

30 KIM, P. *The Hacker Playbook 3: Practical Guide To Penetration Testing*. [S.l.]: Secure Planet LLC, 2018. ISBN-13 978-1980901754.

31 HERZOG, P. Osstmm 2.2–open source security testing methodology manual. *Open source document, www. isecom. org/osstmm*, 2006.

32 RATHORE, B.; BRUNNER, M.; DILAJ, M.; HERRERA, O.; BRUNATI, P.; SUBRAMANIAM, R.; RAMAN, S.; CHAVAN, U. Information systems security assessment framework (issaf). *Draft 0.2 B*, v. 1, p. 2006, 2006.

33 PRATAMA, I. P. A. E.; WIRADARMA, A. A. B. A. Open source intelligence testing using the owasp version 4 framework at the information gathering stage (case study: X company). *International Journal of Computer Network and Information Security*, Modern Education and Computer Science Press, v. 11, n. 7, p. 8, 2019.

34 DALZIEL, H. *Next generation red teaming*. first. 225 Wyman Street, Waltham, MA 02451, USA: Syngress, 2015. ISBN: 978-0-12-804171-0.

35 OAKLEY, J. Improving offensive cyber security assessments using varied and novel initialization perspectives. In: *Proceedings of the ACMSE 2018 Conference*. New York, NY, USA: ACM, 2018. (ACMSE '18), p. 3:1–3:9. ISBN 978-1-4503-5696-1. ISBN 978-1-4503-5696-1. Disponível em: <http://doi.acm.org/10.1145/3190645.3190673>.

36 Henshel, D. S.; Deckard, G. M.; Lufkin, B.; Buchler, N.; Hoffman, B.; Rajivan, P.; Collman, S. Predicting proficiency in cyber defense team exercises. In: *MILCOM 2016 - 2016 IEEE Military Communications Conference*. [S.l.: s.n.], 2016. p. 776–781. ISSN 2155-7586.

37 FERREIRA, H. G. C.; JUNIOR, R. T. de S. Security analysis of a proposed internet of things middleware. *Cluster Computing*, v. 20, n. 1, p. 651–660, Mar 2017. ISSN 1573-7543. Disponível em: <https://doi.org/10.1007/s10586-017-0729-3>.

38 ANTONAKAKIS, M.; APRIL, T.; BAILEY, M.; BERNHARD, M.; BURSZTEIN, E.; COCHRAN, J.; DURUMERIC, Z.; HALDERMAN, J. A.; INVERNIZZI, L.; KALLITSIS, M.; KUMAR, D.; LEVER, C.; MA, Z.; MASON, J.; MENSCHER, D.; SEAMAN, C.; SULLIVAN, N.; THOMAS, K.; ZHOU, Y. Understanding the mirai botnet. In: *26th USENIX Security Symposium (USENIX Security 17)*. Vancouver, BC: USENIX Association, 2017. p. 1093–1110. ISBN 978-1-931971-40-9. Disponível em: <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis>.

39 KREBS, B. Krebsonsecurity hit with record ddos.(2016). *URL https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos*, 2016.

40 SPRING, T.; CARPENTER, K.; MIMOSO, M. Bashlite family of malware infects 1 million iot devices. *Threat Post*, 2016.

41 MALÉCOT, E. L.; INOUE, D. The carna botnet through the lens of a network telescope. In: SPRINGER. *International Symposium on Foundations and Practice of Security*. [S.l.], 2013. p. 426–441.

42 WHITMAN, M. E.; MATTORD, H. J. *Principles of information security 6 ed.* [S.l.]: Cengage Learning, 2016.

43 MITNICK, K. *Ghost in the wires: My adventures as the world's most wanted hacker*. [S.l.]: Hachette UK, 2011.

44 MITNICK, K. D.; SIMON, W. L. *The art of intrusion: the real stories behind the exploits of hackers, intruders and deceivers*. [S.l.]: John Wiley & Sons, 2009.

45 WEISSBRODT, D. Cyber-conflict, cyber-crime, and cyber-espionage. *Minn. J. Int'l L.*, HeinOnline, v. 22, p. 347, 2013.

46 BROWN, G. G.; CARLYLE, W. M.; SALMERON, J.; WOOD, K. Analyzing the vulnerability of critical infrastructure to attack and planning defenses. In: *Emerging Theory, Methods, and Applications*. [S.l.]: Informs, 2005. p. 102–123.

47 SATVAT, K.; HOSSEINI, M.; SHIRVANIAN, M. Camouflaged with size: A case study of espionage using acquirable single-board computers. *arXiv preprint arXiv:1809.04112*, 2018.

48 KNOTT, D. B. A.; MANCUSO, D. V. F.; BENNETT, D. K.; FINOMORE, D. V.; MCNEESE, D. M.; MCKNEELY, M. J. A.; BEECHER, M. M. Human factors in cyber warfare: Alternative perspectives. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, v. 57, n. 1, p. 399–403, 2013. Disponível em: <https://doi.org/10.1177/1541931213571086>.

49 JONES, S.; NEVILLE, S.; CHAFFIN, J. Hackers use tools stolen from nsa in worldwide cyber attack. *Financial Times, 12 May 2017*, 2017.

50 ROHLEDER, R. Hands-on ghidra-a tutorial about the software reverse engineering framework. In: *Proceedings of the 3rd ACM Workshop on Software Protection*. [S.l.: s.n.], 2019. p. 77–78.

51 SHARPE, R. Just what is smb. *Oct*, v. 8, p. 9, 2002.

52 SCAIFE, N.; CARTER, H.; TRAYNOR, P.; BUTLER, K. R. Cryptolock (and drop it): stopping ransomware attacks on user data. In: IEEE. *2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*. [S.l.], 2016. p. 303–312.

53 MOHURLE, S.; PATIL, M. A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, International Journal of Advanced Research in Computer Science, v. 8, n. 5, 2017.

54 PERLROTH, N.; SHANE, S. In baltimore and beyond, a stolen nsa tool wreaks havoc. *New York Times*, v. 25, 2019.

55 DENNING, D. E. Framework and principles for active cyber defense. *Computers Security*, v. 40, p. 108 – 113, 2014. ISSN 0167-4048. ISSN 0167-4048. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0167404813001661>.

56 KAMARA, S.; FAHMY, S.; SCHULTZ, E.; KERSCHBAUM, F.; FRANTZEN, M. Analysis of vulnerabilities in internet firewalls. *Computers Security*, v. 22, n. 3, p. 214 – 232, 2003. ISSN 0167-4048. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0167404803003109>.

57 ZHANG, X.; LI, C.; ZHENG, W. Intrusion prevention system design. In: IEEE. *The Fourth International Conference onComputer and Information Technology, 2004. CIT'04.* [S.l.], 2004. p. 386–390.

58 ROWLAND, C. H. *Intrusion detection system*. [S.l.]: Google Patents, 2002. US Patent 6,405,318.

59 STROM, B. E.; APPLEBAUM, A.; MILLER, D. P.; NICKELS, K. C.; PENNINGTON, A. G.; THOMAS, C. B. Mitre att&ck^{TM}: Design and philosophy. *Technical report*, 2018.

60 HECKMAN, K. E.; WALSH, M. J.; STECH, F. J.; O'BOYLE, T. A.; DICATO, S. R.; HERBER, A. F. Active cyber defense with denial and deception: A cyber-wargame experiment. *Computers Security*, v. 37, p. 72 – 77, 2013. ISSN 0167-4048. Disponível em: <http://www.sciencedirect.com/science/article/pii/S016740481300076X>.

61 AGARWAL, S.; SUREKA, A.; GOYAL, V. Open source social media analytics for intelligence and security informatics applications. In: SPRINGER. *International Conference on Big Data Analytics*. [S.l.], 2015. p. 21–37.

62 INTERPOL. *Terrorists use social media for radicalization, recruitment, funding, planning and execution of terror activities.* 2009. URL:https://www.interpol.int/en/Crimes/Terrorism/Analysing-social-media. Access in 04 apr 2020 19:36.

63 SIMPSON, C. *Science of coercion: Communication research & psychological warfare*. 180 Maiden Lane, Suite 8A New York, NY 10038: Open Road Media, 2015. v. 13. ISBN-13 978-0195102925.

64 QUALTER, T. H. *Propaganda and psychological warfare*. [S.l.]: Pickle Partners Publishing, 2020.

65 SHARP, J. M.; BLANCHARD, C.; KATZMAN, K.; MIGDALOVITZ, C.; PRADOS, A.; GALLIS, P.; RENNACK, D.; ROLLINS, J.; BROWNE, M.; BOWMAN, S. et al. Lebanon: The israel-hamas-hezbollah conflict. In: LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE. [S.l.], 2006.

66 THOMAS, T. L. *Hezballah, Israel, and Cyber PSYOP*. [S.l.], 2007.

67 MONTEIRO, G. A. P.; FREITAS, A. L. P. Análise importância-desempenho aplicada à avaliação da qualidade em serviços de infraestrutura de ti. *Simpósio de Engenharia de Produção-SIMPEP*, v. 22, p. 15, 2015. Av. Eng. Luiz Edmundo Carrijo Coube, 14-01, Bauru - SP. ISSN 1809-7189.

68 Rinaldi, S. M.; Peerenboom, J. P.; Kelly, T. K. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, v. 21, n. 6, p. 11–25, 2001.

69 CASE, D. U. Analysis of the cyber attack on the ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, v. 388, 2016.

70 NASH, T. An undirected attack against critical infrastructure. *Technical Report, US-CERT Control Systems Security Center*, 2005.

71 ROCHA, B.; JUNIOR, R. de S. Identifying bank frauds using crisp-dm and decision trees. *International Journal of Computer Science Information Technology*, v. 2, 10 2010.

72 NUNES, P. A definição de uma estratégia nacional de cibersegurança. *Nação e defesa*, IDN, v. 133, p. 113–127, 2012. Av. António José de Almeida – 1000-042 Lisboa. URL: https://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf. ISSN 0870-757X.

73 MARCELLINO, W.; SMITH, M. L.; PAUL, C.; SKRABALA, L. *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations*. [S.l.]: RAND Corporation, 2017.

74 WEIMANN, G. *Terrorism in cyberspace: The next generation*. [S.l.]: Columbia University Press, 2015.

75 PELINO, E. *TERRORIST INFORMATION OPERATIONS IN CYBERSPACE. THE ISIS CASE: FROM DABIQ TO RUMIYAH*. Tese (Doutorado), 07 2018.

76 YANG, L.; MING, L. X.; HUAN, W. Z.; QIU, W. Y. Design of command effectiveness evaluation software for overseas anti-terrorism operation command system. In: IEEE. *2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*. [S.l.], 2019. v. 1, p. 1161–1166.

77 CEPIK, M. Inteligência e políticas públicas: dinâmicas operacionais e condições de legitimação. *Security and Defense Studies Review*, v. 2, n. 2, p. 246–267, 2002. URL: https://www2.mppa.mp.br/sistemas/gcsubsites/upload/60/Intelig%C3%83%C2%AAncia%20e%20Pol%C3%83%C2%ADticas%20P%C3%83%C2%BAblicas(1).pdf ISSN 1533-2535.

78 VAN HOOREN, J. *THE IMPERATIVE SYMBIOTIC RELATIONSHIP BETWEEN SOF AND CYBER: HOW DUTCH SPECIAL OPERATION FORCES CAN SUPPORT CYBER OPERATIONS*. Calhoun, 2019. Disponível em: <https://calhoun.nps.edu/handle/10945/64086>.

79 MARSH, C.; KIRAS, J.; BLOCKSOME, P. *Special operations research: Out of the shadows*. [S.l.]: Taylor & Francis, 2015.

80 TECNOLOGIA da informação - Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. [S.l.], 2013. ABNT NBR ISO/IEC 27037:2013.

81 SIMãO, A.; SíCOLI, F.; MELO, L.; DEUS, F.; JUNIOR, R. de S. Acquisition and analysis of digital evidence in android smartphones. In: . [S.l.: s.n.], 2011. v. 6, p. 28.

82 KIM, D.; JANG, H.-U.; MUN, S.-M.; CHOI, S.; LEE, H.-K. Median filtered image restoration and anti-forensics using adversarial networks. *IEEE Signal Processing Letters*, IEEE, v. 25, n. 2, p. 278–282, 2017.

83 G1, P. Disponível em:<http://g1.globo.com/sao-paulo/noticia/2016/10/hacker-que-clonou-celular-de-marcela-temer-e-condenado-5-anos-de-prisao.html>. *Acessado em 10/04/2020 as 22:51*, v. 0, 2016.

84 PAYAO, F. *Homem com fotos íntimas de Marcela Temer comprou HD nas ruas de SP*. [S.l.]: Tecmundo, 2016.

85 G1, P. Disponível em:<https://g1.globo.com/sao-paulo/noticia/hacker-condenado-por-chantagear-primeira-dama-disse-ter-audio-que-jogaria-nome-de-temer-na-lama.ghtml>. *Acessado em 11/04/2020 as 11:12*, v. 0, 2016.

86 WILLEMS, C.; HOLZ, T.; FREILING, F. Toward automated dynamic malware analysis using cwsandbox. *IEEE Security & Privacy*, IEEE, v. 5, n. 2, p. 32–39, 2007.

87 SHEN, D.; CHEN, G.; BLASCH, E.; TADDA, G. Adaptive markov game theoretic data fusion approach for cyber network defense. In: IEEE. *MILCOM 2007-IEEE Military Communications Conference*. [S.l.], 2007. p. 1–7.

88 FRITZ, J. R. *China's Cyber Warfare: The Evolution of Strategic Doctrine*. [S.l.]: Lexington Books, 2017.

89 CARDWELL, K. *Building virtual pentesting labs for advanced penetration testing*. [S.l.]: Packt Publishing Ltd, 2014.

90 RAZZAQ, A.; HUR, A.; SHAHBAZ, S.; MASOOD, M.; AHMAD, H. F. Critical analysis on web application firewall solutions. In: IEEE. *2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS)*. [S.l.], 2013. p. 1–6.

91 SOARES, L. F. G.; LEMOS, G.; COLCHER, S. Redes de computadores. *Editora Campus*, 1995.