ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

Cap Com AMILCAR GOROSITO PEDROZO

A IMPORTÂNCIA DO CONHECIMENTO DE REDES DE TECNOLOGIA DA INFORMAÇÃO PARA OS MILITARES DA ARMA DE COMUNICAÇÕES

Rio de Janeiro

2023

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

Cap Com AMILCAR GOROSITO PEDROZO

A IMPORTÂNCIA DO CONHECIMENTO DE REDES DE TECNOLOGIA DA INFORMAÇÃO PARA OS MILITARES DA ARMA DE COMUNICAÇÕES

Trabalho de Conclusão de Curso apresentado à Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do grau especialização em Ciências Militares.

Orientador: Cap Com Rogério Gomes Barbosa Júnior

Rio de Janeiro

2023

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a). Permitida a reprodução parcial ou total, desde que citada a fonte.

P372

Pedrozo, Amilcar Gorosito.
A importância do conhecimento de redes de Tecnologia da Informação para os militares da Arma de Comunicações / Amilcar Gorosito Pedrozo - 2023
57 f. il. color.

Trabalho de Conclusão de Curso - Escola de Aperfeiçoamento de Oficiais - EsAO, Rio de Janeiro, 2023.

1. Arma de Comunicações 2. Redes de Tecnologia da Informação 3. Tecnologia da Informação I Escola de Aperfeiçoamento de Oficiais. II Título.

CDD: 355

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS
(E. A. O./1919)

DIVISÃO DE ENSINO E PESQUISA / CURSO DE COMUNICAÇÕES

Ao Cap Com AMILCAR GOROSITO PEDROZO .

O Presidente da Comissão de Avaliação do TCC, cujo título é A IMPORTÂNCIA DO CONHECIMENTO DE REDES DE TECNOLOGIA DA INFORMAÇÃO PARA OS MILITARES DA ARMA DE COMUNICAÇÕES, informa à Vossa Senhoria o seguinte resultado da deliberação: **APROVADO** com o conceito MUITO BOM.

Rio de Janeiro, 25 de setembro de 2023

ANDERSON GUSTAVO LIMA DOS SANTOS - Maj
Presidente

ROGÉRIO GOMES BARBOSA JÚNIOR - Cap
1º Membro / Orientador

GLAUCO GONÇALVES DA SILVA - Cap
2º Membro

CIENTE: Amilcar Gorosito Pedrozo
AMILCAR GOROSITO PEDROZO - Cap
Postulante

RESUMO

Com os grandes avanços da tecnologia da informação e sua rápida atualização, modernizando, conectando e integrando cada vez mais tudo ao nosso redor, tornou-se de grande importância o conhecimento sobre redes de tecnologia da informação (TI) para militares. A Arma de Comunicações cuja vocação, entre as Armas, Quadros e Serviços, é a mais voltada para a área da tecnologia da informação, precisa acompanhar esses avanços tecnológicos e saber gerenciar e conectar essas novas capacidades para que elas trabalhem como uma rede de informações em apoio a decisão. Dessa forma, tornou-se imprescindível o conhecimento de redes de TI para o comunicante. O presente trabalho tem por objetivo mostrar a importância desse conhecimento para os militares da Arma de Comunicações e porque ele se tornou tão essencial, principalmente, para os comunicantes. A metodologia utilizada para o desenvolvimento foi um estudo descritivo realizado por meio de sites, artigos científicos e outros trabalhos de conclusão de curso.

Palavras-chave: Arma de Comunicações. Redes de Tecnologia da Informação. Tecnologia da Informação.

ABSTRACT

With the great advances in information technology and its rapid updating, modernizing, connecting and integrating everything around us, knowledge about information technology (IT) networks for the military has become of great importance. The Signal Corps branch whose vocation, among Arms, Staff and Services, is the most focused on the area of information technology, needs to keep up with these technological advances and know how to manage and connect these new capabilities so that they work as an information network in decision support. Thus, the knowledge of IT networks for the Signal Corps has become essential. The present work aims to show the importance of this knowledge for the military of the Signal Corps branch and why it has become so essential, especially for the Signal Corps. The methodology used for the development was a descriptive study carried out through websites, scientific articles and other course conclusion works.

Keywords: Signal Corps. Information Technology Networks. Information Technology.

SUMÁRIO

1. INTRODUÇÃO

O Conhecimento em redes de Tecnologia da Informação (TI) adquiriu uma grande importância no século XXI. A necessidade do conhecimento de rede de TI, principalmente para os militares da Arma de Comunicações, tem se mostrado essencial no dia a dia e muito presente no combate moderno. Dessa forma, os comunicantes, que integram a Arma mais vocacionados dentro do Exército Brasileiro (EB) para a área de TI, devem dedicar-se a esse conhecimento e mate-lo o mais atualizado possível.

A redes de tecnologia da informação estão em constante modernização, pois estão em uma busca incansável por melhorias. Para empresas, clientes e fornecedores, a comunicação tornou-se um dos principais fatores de sucesso. A tecnologia de redes, não só a parte física, mas também a parte lógica, vem sendo marcada por sistemas e estruturas cada vez mais complexos e diversificados. As estruturas, tanto físicas quanto lógicas, estão em constante mudanças como atualizações de versões de protocolos, surgimento de novos protocolos mais seguros, novos meios físicos de transmissão como a fibra ótica que, em comparação com o par trançado (cabo azul), possibilita um volume muito superior de tráfego de dados.

> O crescimento implacável das redes e a miniaturização da tecnologia estão levando a uma conectividade mais persistente e confiável e a métodos mais confiáveis de autenticação de usuários. (HIRSCHKORN, 2022, tradução nossa)

Toda essa nova tecnologia, para que seja empregada de uma forma eficiente, necessita de um profissional habilitado que saiba implantar, gerenciar e garantir a segurança e interoperabilidade dos *hardwares* e *softwares* sobre sua responsabilidade.

A área de Tecnologia de Informação tem propiciado um grande aumento na produtividade de quem sabe usufruir dos seus benefícios. Muitas empresas e instituições, nisso se inclui o Exército Brasileiro, aumentaram as suas capacidades de produção de informação e gerenciamento em virtude dos benefícios da TI. Saber tirar proveito dessa vasta área que é a TI, gerenciando as milhares de ferramentas que

são ofertadas e não comprometer a segurança, tornou-se praticamente um desafio para quem trabalha na área.

Junto com os benefícios que a tecnologia trouxe, vieram também perigos como por exemplo os *malwares* que contaminam as redes e outros que comprometem a segurança e o funcionamento das redes de TI.

> A grande ameaça dos malwares advém dos crackers, indivíduos com grande expertise na área cibernética que utilizam seus conhecimentos para realizar atividades maliciosas nas redes de computadores a fim de obter vantagens individuais (CONCEIÇÃO, 2017).

De acordo com Junior (2020), só em 2019, o Brasil teve mais de 24 bilhões de incidentes de segurança cibernéticas, uma média de 65 milhões ao dia. Ele chama a atenção para o grande número de ataque que cresceu, principalmente, no período da pandemia. Isso ocorreu por fragilidade em redes como:

> [...] redes que não fazem uso da certificação, os roteadores abertos, mais fáceis de configurar, e o maior volume de conexões em todas as esferas, são possíveis portas abertas para a invasão dos criminosos. (JUNIOR, 2020)

Com isso, saber estruturar uma rede de computadores, administrá-la da maneira correta e garantir sua segura é essencial para não ser alvo das inúmeras ameaças que vagam pela Internet.

Para que isso ocorra, o comunicante precisa acompanhar o surgimento dos novos sistemas e ferramentas para poder criar as melhores condições para atender as demandas do Comando, particularmente do Sistema de Comunicações. (BRASIL, 2020)

> A moderna comunicação militar também desenvolveu softwares de consciência situacional, que atualizam, instantaneamente, o chefe militar com informações do teatro de operações, bem como proporcionam a troca de informações entre os diversos escalões. Essa predominância de emprego de sistemas computadorizados e softwares nas comunicações militares em um ambiente operacional volátil, incerto, complexo e ambíguo, como o do combate moderno, traz um novo desafio: a Defesa Cibernética. (EXÉRCITO, 2022, p. 3).

Dessa forma, esse estudo busca analisar a importância do conhecimento de redes de Tecnologia de Informação para o militar da Arma de Comunicações, identificado os possíveis empregos em ambientes de guerra e não guerra em prol da

segurança das OM e de um melhor desempenho nas atividades de Comando e Controle (C^2).

1.1 PROBLEMA

Durante a formação militar, muitos militares da Arma de Comunicações não desenvolvem de maneira eficiente os seus conhecimentos de rede de tecnologia da informação e formam-se sem saber a importância da sua falta. Além disso, depois de formados, não conseguem enxergar a importância desse conhecimento ou possuem dificuldade para adquiri-lo.

Se pensarmos como Pinheiro:

> O chamado Conflito de 4ª Geração, também identificado como Conflito Irregular Assimétrico, característico da Guerra Irregular, passa por um efetivo processo de evolução, no qual a Tecnologia da Informação é fator preponderante. (PINHEIRO, 2008, p. 1)

Nesse contexto, ele ainda destaca as Operações de Informação.

> Essas, por sua vez, englobam cinco grandes competências: as Operações em Rede Computadorizada; a Guerra Eletrônica; a Simulação Militar; as Operações de Segurança e as Operações Psicológicas. (PINHEIRO, 2008, p. 1).

Isso mostra que o conhecimento de TI se tornou fundamental e o conhecimento de redes de TI é apenas uma das muitas partes.

Dessa forma, para dar mais ênfase ao conhecimento de redes e destacar sua importância, Da Silva (2014, p.195) afirma:

> Cada vez mais computadores, seus equipamentos de interconexão, sistemas de comando, controle, comunicações e informação (C^3I) e sistemas de apoio à decisão compõem o espaço cibernético militar, em que a informação é o objetivo maior. Dessa forma, esse espaço se tornou fundamental na guerra, em decorrência da grande importância militar dos computadores e de suas redes para a circulação de ordens ou informações.

No Exército Brasileiro a gestão de TI nas Organizações Militares (OM) é realizada, geralmente, pela Seção de Informática que costuma empregar militares comunicantes, devido à proximidade da vocação da Arma, e outros militares com conhecimento de TI.

Assim, é oportuno problematizar a questão: qual a importância do conhecimento de redes de tecnologia da informação para os militares da Arma de Comunicações no século XXI?

1.2 OBJETIVO

O objetivo a ser alcançado nesse trabalho foi divido em objetivo geral, que traz a principal finalidade deste trabalho, e em objetivos específicos, que servem para delinear os estudos a serem desenvolvidos.

1.2.1 **Objetivo Geral**

O objetivo geral é verificar a importância do conhecimento de Redes de Tecnologia da Informação para os militares da Arma de Comunicações no século XXI.

1.2.2 **Objetivos Específicos**

Foram observados os seguintes objetivos específicos de modo a delinear a consecução deste estudo e permitir um encadeamento lógico do raciocínio, os quais são transcritos abaixo:

- identificar o emprego da tecnologia da informação pelos militares da Arma de Comunicações;

- citar as possibilidades de emprego das redes de tecnologia de informação e suas ferramentas em ambientes de guerra e não guerra;

- analisar a importância do conhecimento sobre as redes de tecnologia da informação para os militares da Arma de Comunicações no século XXI.

1.3 HIPÓTESES

Trabalhar com redes de tecnologia da informação (TI) envolve vários conhecimentos da área de informática. A área da TI é muito vasta, possuindo diversos *hardwares* e *softwares*. Esta pesquisa pretende identificar a importância do conhecimento de redes de TI para os militares da Arma de Comunicações e quais os reflexos desse conhecimento para seu desempenho profissional.

Uma hipótese que norteia a pesquisa, portanto, consiste em se verificar se esse conhecimento é importante para os militares da Arma de Comunicações e se possui empregabilidade para eles. Caso haja, em que medida é importante para o desempenho profissional do comunicante.

Uma segunda hipótese da pesquisa é verificar se o conhecimento redes de TI não possui importância para o militar da Arma de Comunicações e, dessa forma, não trazendo benefícios para o seu desempenho profissional.

1.4 JUSTIFICATIVAS

Quando se observa outros exércitos como por exemplo o exército americano, ele possui em suas opções de carreira "*Tecnology and Networking*", que são os "Especialistas em tecnologia da informação (TI) e redes que mantêm dispositivos, solucionam problemas de mau funcionamento e executam instalações de rede." (ARMY NATIONAL GUARD, tradução nossa). Dessa forma, preparam militares focados em redes de TI.

Para o Exército Brasileiro, o militar que no combate desempenha essa função é o comunicante. De acordo com o Manual de Campanha EB70-MC-10.241 As Comunicações na Força Terrestre:

> “Cada escalão da F Ter possui seu elemento de comunicações, que tem por missão o planejamento, a instalação, a exploração, a manutenção e a proteção das comunicações, no seu nível, bem como prover a segurança física das suas áreas e instalações.” (BRASIL, 2018, p. 16).

Para que isso ocorra de maneira eficiente, os militares da Arma de Comunicações precisam acompanhar os avanços tecnológicos ligados às áreas de telecomunicações e da tecnologia da informação.

O crescente avanço tecnológico impõem aos militares comunicantes que dominem certas áreas do conhecimento de Tecnologia da Informação e Comunicação (TIC), pois a área de TI é muito vasta. Um desses conhecimentos, que se tem mostrado de extrema importância, é o de redes de TI.

O avanço tecnológico e a integração dos meios de TI pela rede, acabou criando vários desafios para os comunicantes como por exemplo o ciberespaço. Esse novo ambiente formado com base nas redes de TI, tornou um importante meio de transmissão de dados. De acordo com Abdalla (2021, p. 2):

> Atualmente, o ambiente cibernético das redes de transmissão de dados é o principal vetor de circulação de informações governamentais ostensivas ou sigilosas. É por meio dessas redes que circulam as decisões políticas e estratégicas, bem como as ordens das operações militares.

Com isso, a relevância do trabalho a ser desenvolvido se observa no Plano Estratégico do Exército 2020-2023, mais precisamente, nos Objetivo Estratégico do Exército 4 e 7 (OEE 4 e OEE 7), que aborda a implantação do Setor Cibernético no Exército Brasileiro e a Gestão Estratégica de Tecnologia da Informação e Comunicações (TIC). Esses OEE abordam de maneira significativa a área de redes de TI.

Nesse sentido, o presente trabalho pretendeu verificar a importância do conhecimento de redes de TI para os militares da Arma de Comunicações e o quanto isso pode impactar no seu desempenho profissional.

2. REVISÃO DE LITERATURA

2.1 DELIMITAÇÃO DO TEMA

Esta pesquisa trata sobre a importância do conhecimento de Redes de TI para os militares da Arma de Comunicações no desempenho de suas funções, abordando informações, preferencialmente, do período após o ano de 2015. Nesse caso, foca-se na importância que os militares de comunicações devem dar para desenvolver esse conhecimento e como isso reflete no exercício de sua função. Assim, o trabalho se limitou em destacar a importância do conhecimento de redes de TI e o nos seus possíveis empregos pelos comunicantes.

2.2 REVISÃO DE LITERATURA

2.2.1 **Tecnologia da Informação e Comunicação (TIC)**

O conhecimento de Tecnologia da Informação (TI) e o domínio sobre essa área tem se mostrado muito importante na sociedade atual. Saber criar, administrar e gerenciar, desde pequenas redes de computadores até uma grande rede corporativa, entender sobre protocolos e o funcionamento de todos os dispositivos interligados em uma rede, tornou-se fundamental.

Atualmente pode-se encontrar muito conteúdo em livros, vídeos, trabalhos e páginas na internet que se propõem a oferecer subsídios para desenvolver o conhecimento em rede de TI, explicando os mais diversos tipos de redes de TI, seus protocolos e aplicações. Também há variada oferta de cursos, divulgados na mídia de um modo geral. Todos esses conteúdos oferecem possibilidades de melhoria no domínio sobre o conhecimento de TI, aperfeiçoando o desempenho profissional. Parte-se do pressuposto de que o conhecimento de TI pode ser aprendido e desenvolvido.

A literatura a respeito de TI é volumosa, variada e possui vários elementos. Valle (2002, p. 2) traz uma definição de Morton (1991) sobre tecnologia de informação:

> Segundo Morton, tecnologia da informação é composta dos seguintes elementos: hardware, software, redes de comunicação, workstation (CAD, CAM, CIM etc.), robótica e os chips inteligentes.

De acordo com Grosso (2019, p. 4) pode-se inferir que TI:

> [...] baseia-se no desenvolvimento, no estudo e na prática de sistemas de computador, especialmente no tocante à união de hardware, software e peopleware, definindo rapidamente a sua atividade na evolução da computação apoiada em redes de comunicação.

Um outro conceito de Mendes (2022) sobre TI:

> Ainda que possa ser compreendida de várias formas, a TI é entendida como o conjunto de todas as atividades e soluções produzidas por meio de recursos tecnológicos da computação para realizar o armazenamento, processamento, utilização e transmissão da informação. Para a informática, a informação será um dado contextualizado do qual alguma tomada de decisão poderá ser feita.

Algar Telecom (2022) traz como forma de complemento para essas definições esta visão:

> ✓ na indústria, as TICs têm sido pensadas mais no sentido de soluções de automação;
> ✓ no comércio, como ferramentas integradas de gestão;
> ✓ para as fintechs, as TICs propõem segurança para lidar com o Big Data gerado intensamente. (TELECOM, 2022)

Pode-se encontrar em vários trabalhos como o de Joffree Ferreira Abdalla (A atuação do Exército Brasileiro para o domínio do espaço cibernético e Domínio do espaço cibernético por um país: uma análise da presença do Exército Brasileiro no domínio Cibernético), Alvaro de Souza Pinheiro (A Tecnologia da Informação e a Ameaça Cibernética na Guerra Irregular do Século XXI), Júlio Cezar Barreto Leite da Silva (Guerra Cibernética: A guerra no Quinto Domínio, conceituação e princípios), todos autores militares, fontes que destacam atividades importantes que são realizadas em ambientes de redes de TI.

A Tecnologia da Informação envolve uma série de atividades e soluções que utilizam recursos computacionais com objetivos e finalidades que podem ser:

- ✓ obtenção;
- ✓ armazenamento;
- ✓ proteção;
- ✓ processamento;
- ✓ acesso;
- ✓ gerenciamento;
- ✓ uso de informações e dados de uma pessoa, seja ela física ou jurídica.

O profissional de TI é o indivíduo responsável por cuidar desse vasto campo tecnológico em sua organização. Ele é o responsável por propor melhorias e soluções tecnológicas para sua empresa e melhorar seus *softwares* e *hardwares* de modo a mate-los sempre atualizados e em condições de prover os serviços necessários sem interrupções e com segurança.

2.2.2 **Ferramentas de Tecnologia da Informação e Comunicação**

Quando se trata de ferramentas de rede de Tecnologia da Informação (TI), atualmente existem inúmeras opções disponíveis para os comunicantes. Essas ferramentas podem ser usadas para aumentar a eficiência, eficácia e segurança das redes de TI, bem como para auxiliar no cumprimento das atividades militares. Algumas dessas ferramentas incluem programas de monitoramento de rede, firewalls, sistemas de detecção de intrusão, software de gerenciamento de configuração, entre outros.

Os programas de monitoramento de rede permitem aos comunicantes acompanhar o desempenho da rede em tempo real e identificar possíveis problemas antes que eles afetem o funcionamento da rede. Os firewalls ajudam a proteger a rede contra ameaças externas, bloqueando o tráfego não autorizado e permitindo apenas o tráfego legítimo. Os sistemas de detecção de intrusão monitoram a rede em busca de atividades suspeitas e alertam os comunicantes quando algo fora do comum é detectado. O software de gerenciamento de configuração ajuda a manter a configuração da rede atualizada e consistente, evitando problemas causados por configurações incorretas.

É importante que os comunicantes estejam familiarizados com essas ferramentas e saibam como usá-las adequadamente para garantir o bom

funcionamento das redes de TI. Além disso, é fundamental manter-se atualizado sobre as novidades e tendências na área de TI, para que possam continuar aprimorando suas habilidades e conhecimentos.

Entre as várias ferramentas existentes, podemos citar como exemplo a ferramenta Zabbix, cuja utilidade é abordada por Denis Lucio de Lima (2020) em seu Trabalho de Conclusão de Curso sobre sua utilização na prevenção a sinistro de rede. A ferramenta Zabbix para o gerenciamento de redes é um software estável e apresenta relatórios muito bons. A ferramenta permite ainda o monitoramento a dispositivos remotos com ou sem o uso de agentes instalados, monitoramento de máquinas virtuais e de aplicações web (Figura 1). (SOUZA, 2017)

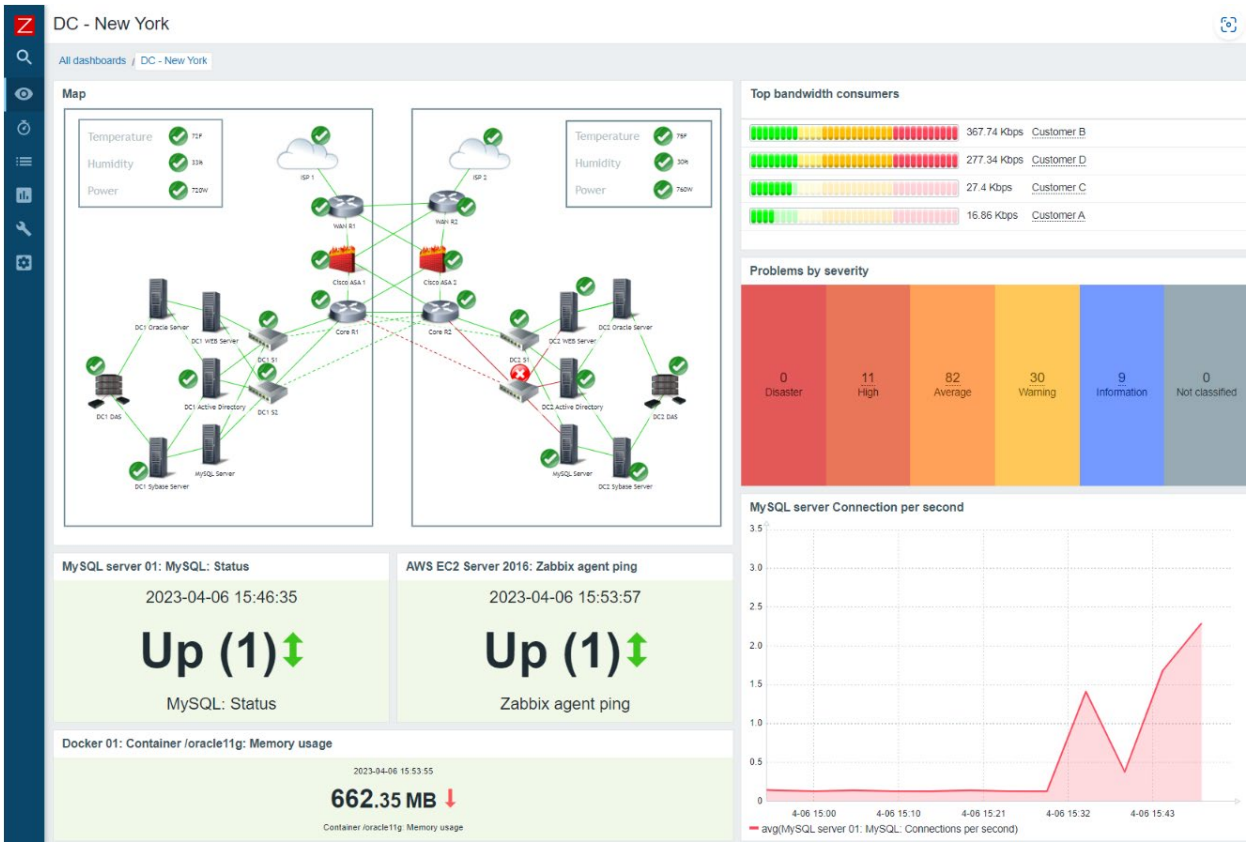

FIGURA 1 – Tela de monitoramento de rede Zabbix
Fonte: Website Zabbix

Com a implantação do Zabbix para monitorar uma rede, é evidente que a equipe de TI terá mais recursos para realizar o suporte e o monitoramento da rede e seus ativos. Isso auxiliará na atuação de forma corretiva e preventiva sobre os ativos monitorados, garantindo a continuidade e segurança dos serviços.

De Lima (2020, p. 22) ainda conclui:

> [...] este estudo deixa ainda evidente a necessidade de toda OM ter uma ferramenta de gerenciamento e monitoramento de ativos de rede, para promover o auxílio necessário aos integrantes da equipe de TI, na tomada de decisão, não somente de forma corretiva, mas preventiva.

Cabe também destacar o trabalho realizado por JÚNIOR (2018, p. 8) sobre monitoração de sistemas em que ele destaca:

> As empresas e organizações estão, cada vez mais dependentes dos sistemas de Tecnologia Informação e Comunicações (TIC). O Exército Brasileiro, como organização também faz uso de sistemas para automatizar, gerenciar, acompanhar e melhorar seus processos e informações

Um outro software utilizado é o PROXMOX que “é uma plataforma de virtualização *open source* para executar máquinas virtuais e contêineres” (NOTO, 2022). O PROXMOX nasceu com um dos objetivos de gerenciar máquinas virtuais (VM) por meio de uma interface web, com base na distribuição Debian GNU/Linux, facilitando a administração de VM. Esta ferramenta permite criar uma rede com várias máquinas virtuais e cada uma rodando um serviço diferente ou vários serviços em uma mesma máquina. Ela ajuda a diminuir as necessidades de manutenção de *hardware* e, também, aumenta a segurança por poder isolar os serviços. O PROXMOX possibilita a criação de placas de redes virtuais em apenas uma placa de rede física e, para usuários mais avançados, existe a opção de configurar o bonding que é a utilização de duas placas de redes para o mesmo servidor. A ferramenta ainda traz funções como backup, administração baseada em funções, autenticação realms, firewall integrado, linha de comando, sistema de arquivos de cluster, entre outras funcionalidades (Figura 2).

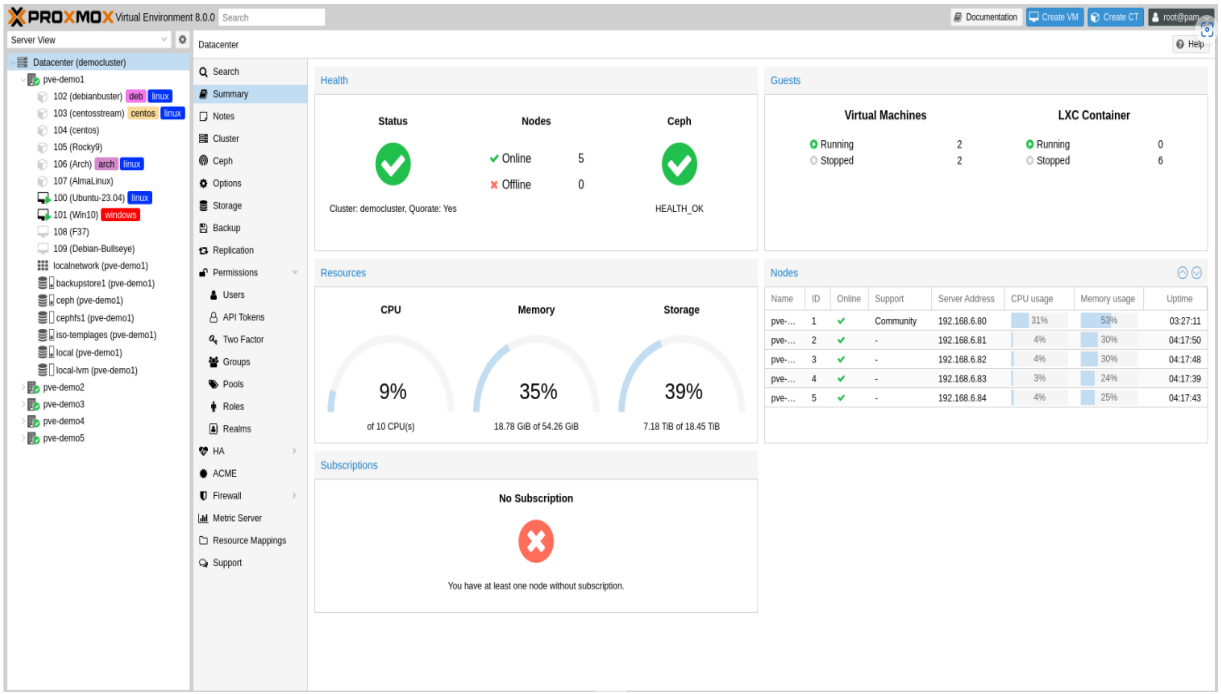

FIGURA 2 – Tela de gerenciamento do PROXMOX
Fonte: Website PROXMOX

A tecnologia permitiu aproximar as pessoas e um recurso que foi muito utilizado por empresas e instituições para reuniões, principalmente durante a pandemia, foi a videoconferência. Nesse quesito, pode-se mencionar o OpenMeetings.

> O OpenMeetings é uma plataforma open source, escrita em java, para realização de apresentações/videoconferências, que disponibiliza um conjunto de ferramentas colaborativas que garantem certamente a melhor produtividade das equipas de trabalho. (PPLWARE, 2018)

O OpenMeetings possibilita ao usuário criar um servidor para videoconferência, a plataforma possibilidade vários recursos como o sistema de moderação, gravação, desenhar e realizar apontamentos em documentos compartilhados, compartilhar tela, chat e outros (Figura 3).

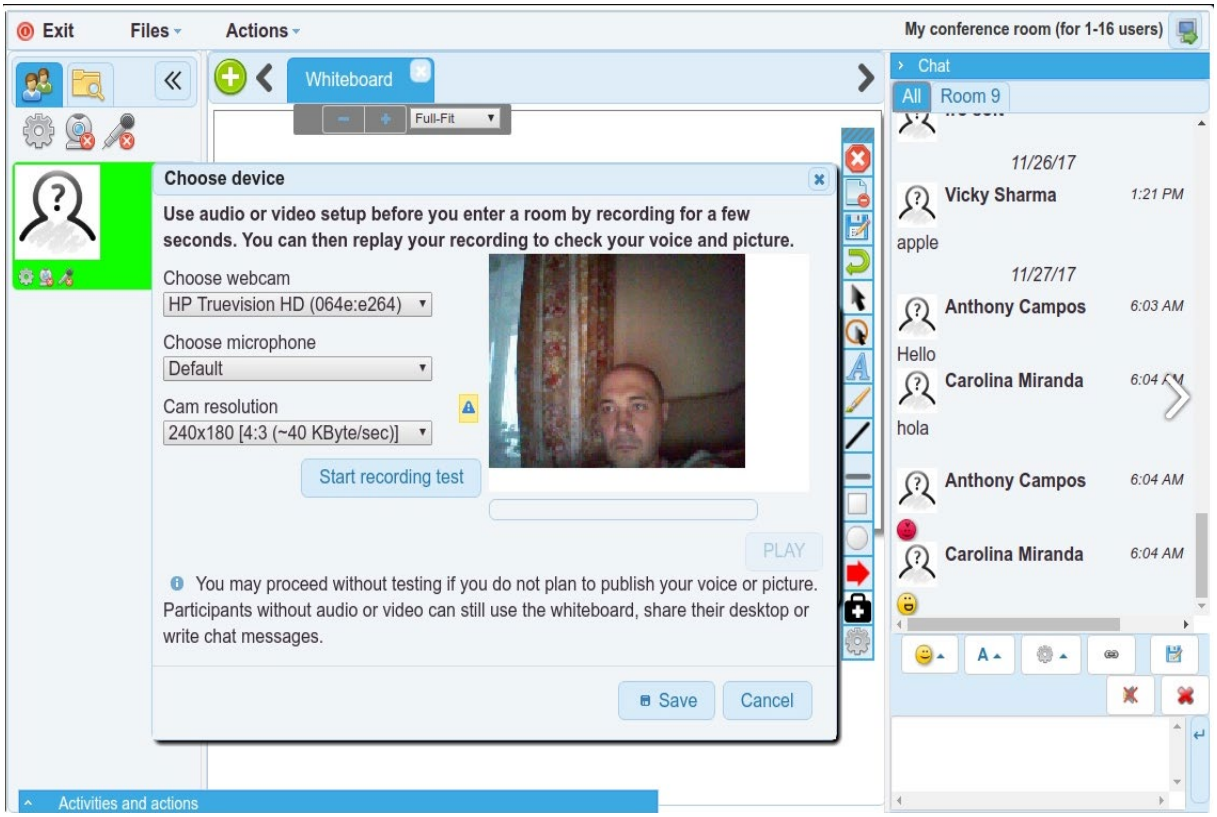

FIGURA 3 – Conferência Web
Fonte: PPLWARE (2018)

Quando se fala de ferramentas de TI não se pode esquecer da necessidade do acesso remoto. Um *software* livre que se pode destacar é o Remmina que já vem integrado ao sistema operacional Linux Ubuntu, distribuído pela Canonical e muito utilizado em computadores do Exército Brasileiro.

> **Remmina** é um cliente de desktop remoto gratuito e de código aberto, rico em recursos e poderoso para Linux e outros sistemas semelhantes ao Unix, escrito em GTK+3. Destina-se a administradores de sistema e viajantes, que precisam acessar remotamente e trabalhar com muitos computadores. (PT.LINUX)

O Remmina permite ao administrador da rede acessar e gerenciar máquinas remotamente (Figura 4), podendo dar suporte e solucionar problemas sem se deslocar até o usuário. Esse software suporta vários recursos como RDP, VNC, NX, XDMCP e SSH e tem vindo já disponível em distribuições Linux Ubuntu que é um distro muito utilizada nos computadores do Exército Brasileiro por ser de licença gratuita. Uma das limitações desse programa foi ter o seu desenvolvimento apenas para distribuições Linux.

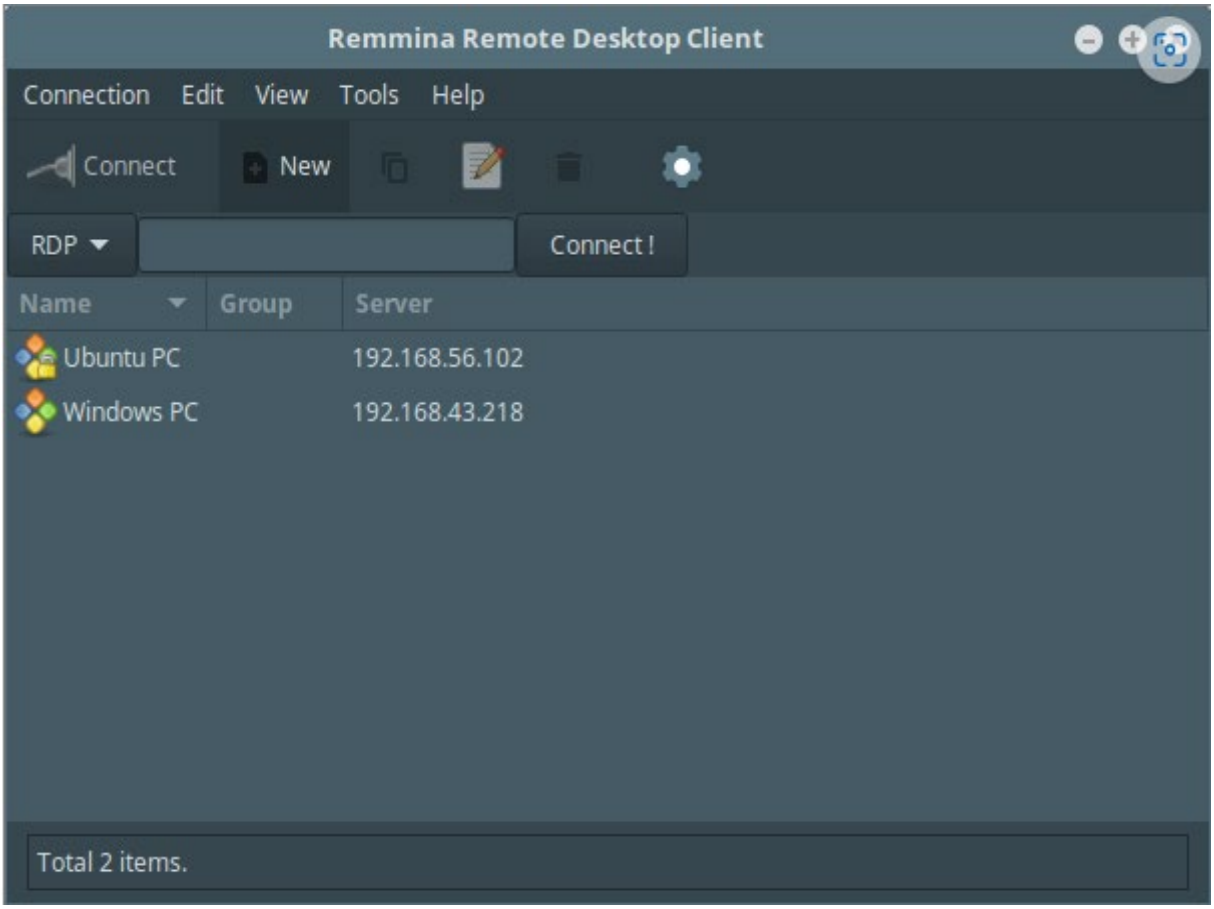

FIGURA 4 – Tela Remmina
Fonte: PT.LINUX

O Zimbra Collaboration é uma plataforma de código aberto que oferece funcionalidades como e-mail, bate-papo e videoconferência (Figura 5). Com ele, é possível criar e compartilhar calendários, gerenciar listas de contatos, armazenar e compartilhar arquivos, entre outras funções. A plataforma é altamente personalizável e pode ser integrada com outras soluções para atender às necessidades específicas de cada organização.

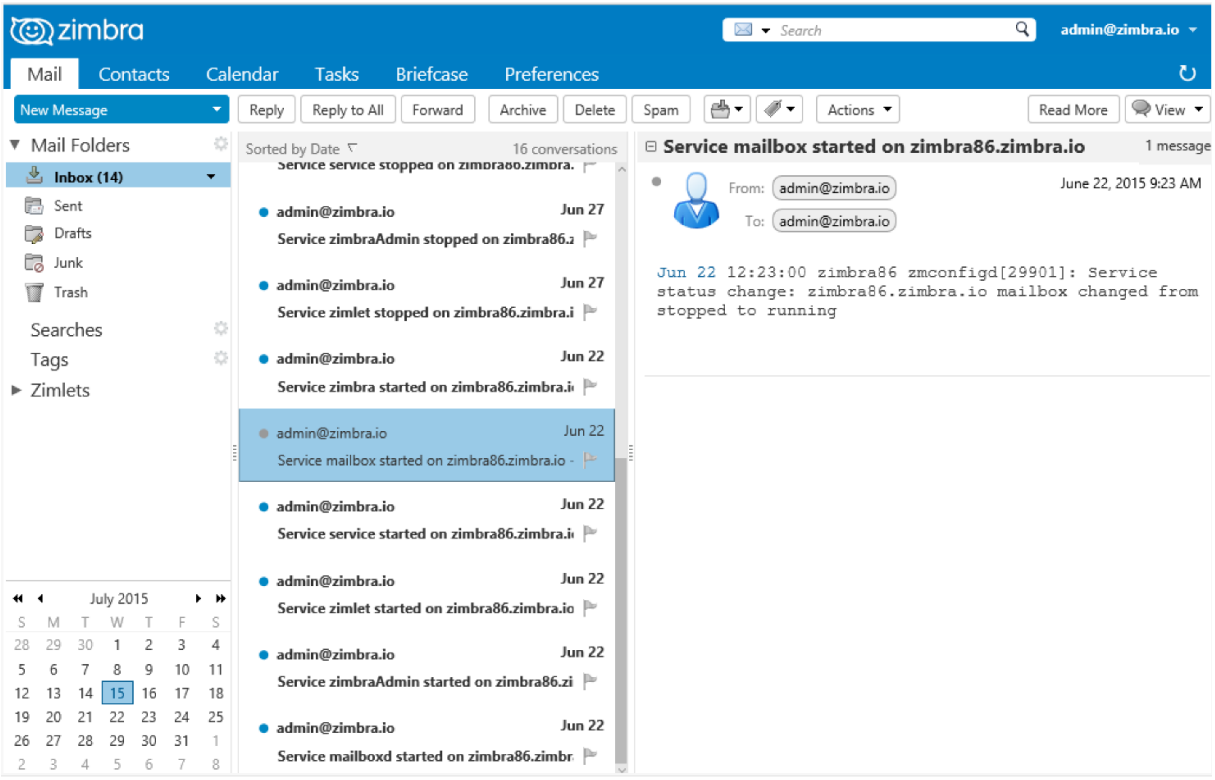

FIGURA 5 – Tela Zimbra
Fonte: Wiki.zimbra

As ferramentas mencionadas anteriormente, Zabbix, PROMOX, OpenMeetings, Remmina e Zimbra, destacam-se por serem softwares open source, ou seja, são softwares de código aberto. Isso significa que o seu código fonte é acessível e pode ser adaptado conforme as necessidades do usuário. Além disso, esses softwares não geram custos de licença e não possuem restrições de uso. A natureza open source dessas ferramentas permite que elas sejam altamente personalizáveis e flexíveis, permitindo que os usuários, no caso o Exército Brasileiro, crie soluções personalizadas para atender às suas necessidades específicas. Além disso, a comunidade open source é altamente colaborativa e oferece suporte e recursos para ajudar a aproveitar ao máximo essas ferramentas. Isso torna essas ferramentas soluções de tecnologia acessíveis e flexíveis.

2.2.3 **Redes de Tecnologia da Informação no Exército Brasileiro e o domínio cibernético**

No Exército Brasileiro (EB), a Arma de Comunicações é a principal responsável pelo Comando e Controle (C^2) nas operações. O Manual de Campanha EB20-MC-10.205 Comando e Controle (2015, p. 43) define os Sistemas de Tecnologia da Informação para C^2 ($STIC^2$) como:

> [...] os recursos de Tecnologia da Informação (TI), constitutivos do sistema de C², que proporcionam ferramentas por meio das quais as informações são coletadas, monitoradas, armazenadas, processadas, fundidas, disseminadas, apresentadas e protegidas.

Ao observar-se o sistema de comunicação do EB, destaca-se a Rede Operacional de Defesa que é utilizada para o tráfego de informações em operações, proporciona acesso aos sistemas e aos serviços hospedados no Centro de Comando e Controle do Ministério da Defesa (CC^2MD), que fornece como principais serviços:

> a) acesso à ROD;
> b) voz sobre IP (VoIP);
> c) correio eletrônico operacional;
> d) serviço de transferência de arquivos (FTP);
> e) rede privada virtual (VPN);
> f) acesso às redes internas de comunicações e de dados das FA;
> g) acesso seguro à internet;
> h) sistema de videoconferência; e
> i) sistemas de apoio à decisão. (BRASIL, 2015)

Os serviços mencionados anteriormente estão diretamente relacionados as de Redes de Tecnologia de Informação.

Uma função desempenhada pelos oficiais da Arma de Comunicações nas OM em que servem é a de Oficial de Informática. Isso ocorre porque é previsto que cada OM possua um Oficial de Informática, sendo ele, o oficial de comunicações, a pessoal geralmente mais apta a ser a responsável pela parte física e lógica de TI da OM, tendo em vista a vocação da Arma para esse lado tecnológico.

> Art. 45. O Oficial de informática é o encarregado do material e infraestrutura das redes de informática da unidade e o responsável pela eficiência e continuidade de seu funcionamento.
> Art. 46. Ao O Infor incumbe:

> I - manter-se atualizado em relação às normas e legislação, em vigor, relativas ao assunto de sua competência e zelar pelo seu cumprimento;
> II - inventariar periodicamente todo o material (hardware e software) da OM;
> III - controlar os recursos de informática existentes, de acordo com a legislação específica;
> IV - estar em condições de informar à Diretoria de Material de Comunicações, Eletrônica e Informática o resultado do inventário do material de informática, quando solicitado;
> V - organizar e manter atualizada a pasta de licenças de software, com os programas em uso na unidade, em estreita ligação com a Fisc Adm;
> VI - propor ao Cmt, Ch ou Dir da OM, medidas para o descarte de hardware e software obsoletos e em desuso;
> VII - estimular o uso de software livre, consoante as orientações do Governo Federal e do Departamento de Ciência e Tecnologia;
> VIII - propor ao Cmdo da OM e supervisionar a realização de treinamento adequado aos usuários e técnicos de informática da unidade;
> IX - propor, difundir e implantar normas de segurança da informação na sua OM, conforme orientações do Cmt U e do Departamento de Ciência e Tecnologia;
> X - assessorar nos processos de aquisição e recebimento de material ou serviço de informática na unidade, segundo critérios de economicidade e adequação às reais necessidades da OM;
> XI - integrar, tanto quanto possível, as atividades de informática e comunicações, no preparo e emprego operacional da unidade, em estreita ligação com o O Com Elt;
> XII - na OM em que existir rede local de computadores e/ou computadores com acesso à Internet, orientar as atividades ligadas ao uso adequado desses recursos, principalmente nos aspectos
> relacionados à segurança da informação;
> XIII - manter atualizados os sítios da Internet de responsabilidade de sua OM; e
> XIV - suprir a eventual carência de pessoal especializado da unidade na área de Informática, com solicitação de apoio à seção correspondente no escalão superior. (BRASIL, 2008, p. 8)

Para o desenvolvimento de operações militares, o militar recebe instrução de como utilizar a Instrução para Exploração das Comunicações (IE Com Elt). Esse documento destina-se ao controle técnico e a coordenação dos órgãos de comunicações que servem ao mesmo comando. (BRASIL, 1995)

Conforme ocorrem os avanços tecnológicos, esse documento tem se tornado cada vez mais complexo, devido a quantidade de meios de Tecnologia da Informação que cada vez mais incorporam os meios de comunicações do Exército Brasileiro.

Para a realização da montagem da rede de TI de um centro de operações, é necessário consultar esse documento e nele é possível se deparar com diversos IP (Internet Protocol), divisão de redes, configurações para servidores VoIPs (Voice Over Internet Protocol) e outras informações de redes de Tecnologia da Informação que, para um indivíduo com pouco conhecimento de TI, pode passar dificuldade para compreender ou, até mesmo, não conseguir montar e configurar a rede por falta de conhecimento específico na área de informática.

Quando se observa uma Viatura de Comando e Controle (VCC), como o Módulo de Telemática Operacional (MTO), que surgiu com o projeto Sistema Integrado de Monitoramento de Fronteira (SISFRON), que foi criado por meio da Diretriz de Implantação, publicada na Portaria nº 193 do Estado Maior do Exército (EME), de 22 de dezembro de 2010, e faz parte do Sistema de Comando e Controle da Força Terrestre (SC2FTer), tem por objetivo dotar o Exército de meios para melhorar a presença e vigilância de áreas de interesse do Território Nacional, particularmente na faixa de fronteira. Nessa VCC percebe-se que ela integrou várias capacidades (Figura 5) que se interconectam por meio de rede de TI. Além de contar com Telefones VoIP do modelo Cisco IP Phone 7945 e notebooks robustecidos do modelo CF-31 para operação em bancada interna do shelter.

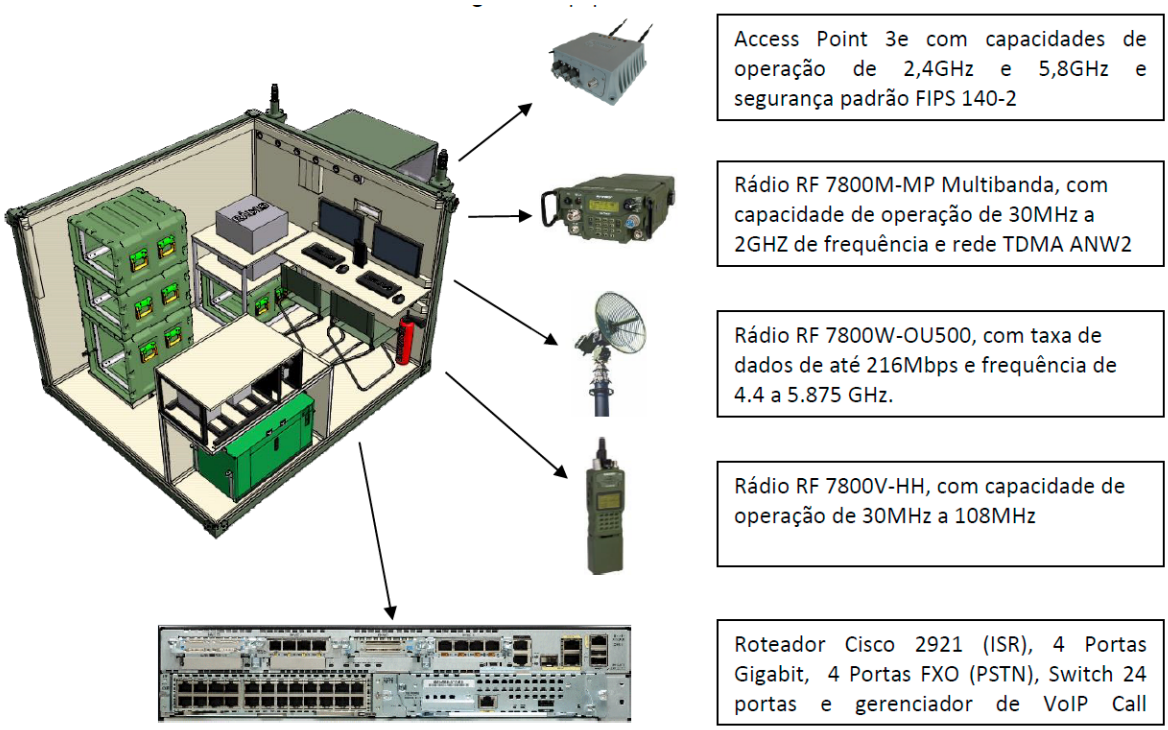

Figura 5 – Equipamentos do MTO
Fonte: HARRIS, 2013

Nessa VCC, o “cérebro” dela é o roteador Cisco 2921 que possui a capacidade para inúmeras configurações de IP e protocolos. Porém para utilizar tais capacidades ao máximo, o operador demanda um grande conhecimento de redes de TI e outros ainda mais específicos sobre o roteador Cisco, demonstrando a importância do conhecimento de TI pelo militar operador/configurador. É possível verificar na figura 6 uma possível configuração de rede para o emprego desse equipamento, em que se

pode verificar a necessidade do conhecimento de redes IP e suas divisões por máscaras de redes.

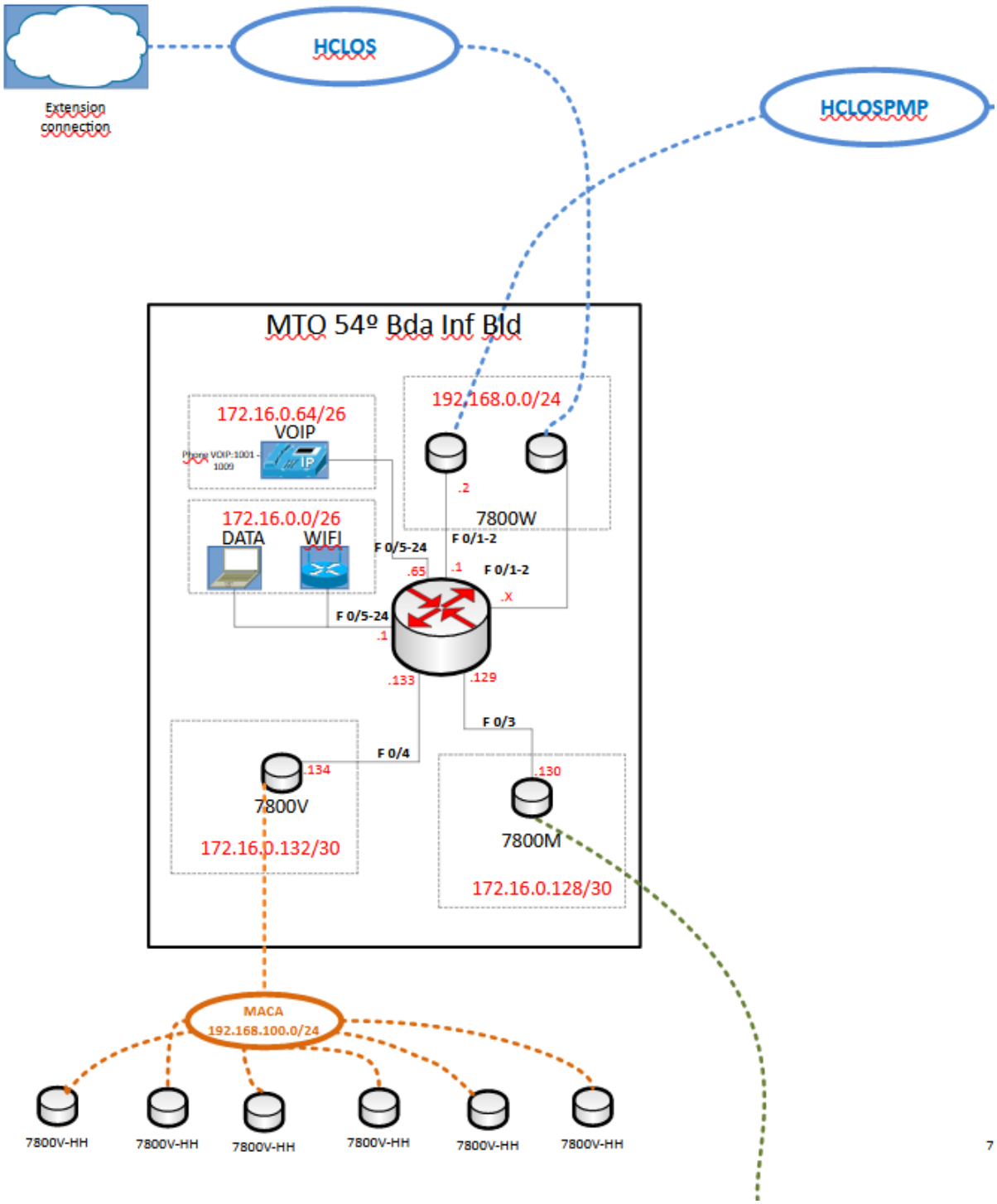

FIGURA 5 – Configuração de um MTO
Fonte: o autor

A Escola de Comunicações (EsCom), Escola Coronel Hygino Corsetti, é responsável por realizar especializações de militares do Exército Brasileiro na área de Comunicações. Ela possui a missão de:

> Habilitar, conforme as necessidades do Exército Brasileiro, profissionais militares a exercerem, com competência, as atribuições do cargo a que se destinam, especialmente na área de Comunicações, dentro das normas de ensino do Exército, realizando pesquisas para contribuir com o desenvolvimento da doutrina de emprego das Comunicações e da manutenção de seus diversos meios. (ESCOLA DE COMUNICAÇÕES)

A EsCom possui uma parceria com instituições públicas e privadas, a fim de oferecer cursos de Redes de Computadores, Tecnologia da Informação e Comunicações (TIC) e Segurança da Informação e Comunicações (SIC). Os cursos são disponibilizados para o as Forças Armadas e, entre os cursos ofertados, pode-se destacar alguns cursos como os da Academias CISCO que possuem uma carga horário de 70 horas e os seguintes objetivos conforme o curso:

> Networking Essentials:
> - Planejar e instalar uma rede residencial ou de pequena empresa e conectá-la à Internet.
> - Desenvolver o pensamento crítico e as qualificações profissionais de resolução de problemas usando o Cisco Packet Tracer.
> - Pratique verificar e solucionar problemas de rede e de conectividade à Internet.
> - Reconhecer e mitigar ameaças à segurança em uma rede residencial.
>
> CCNA: Introduction to Networks
> - Crie LANs simples, faça configurações básicas para roteadores e switches e implemente esquemas de endereçamento IPv4 e IPv6.
> - Configure roteadores, switches e dispositivos finais para fornecer acesso a recursos de rede locais e remotos e permitir a conectividade completa entre dispositivos remotos.
> - Desenvolva o pensamento crítico e as qualificações profissionais de resolução de problemas usando equipamentos reais e o Cisco Packet Tracer.
> - Configure e solucione problemas de conectividade de uma pequena rede usando as melhores práticas de segurança.
>
> CCNA 7: Switching, Routing, and Wireless Essentials
> - Trabalhe com roteadores, switches e dispositivos sem fio para configurar e solucionar problemas de VLANs, LANs sem fio e roteamento entre VLANs.
> - Configure e solucione problemas de redundância em uma rede de switches usando STP e EtherChannel.
> - Desenvolva o pensamento crítico e as qualificações profissionais de resolução de problemas usando equipamentos reais e o Cisco Packet Tracer.
> - Explique como oferecer suporte a redes disponíveis e confiáveis usando protocolos de redundância de primeiro salto e endereçamento dinâmico.

> CCNA 7: Enterprise Networking, Security, and Automation
> - Trabalhe com roteadores e switches usando o OSPF em redes ponto a ponto e multiacesso.
> - Reduza as ameaças e aumente a segurança da rede usando as listas de controle de acesso e as melhores práticas de segurança.
> - Desenvolva o pensamento crítico e as qualificações profissionais de resolução de problemas usando equipamentos reais e o Cisco Packet Tracer.
> - Entenda a virtualização, a SDN e como as ferramentas de gerenciamento de configuração e APIs permitem a automação de rede. (NETACAD)

Os cursos mencionados são todos realizados de forma EaD (Ensino a Distância), e fornecem uma excelente capacitação em redes para todos os militares, independente da Arma, Quadro ou Serviço.

A escola também conta com cursos livres da Escola de Comunicações e da Escola Nacional de Defesa Cibernética no seu portal na Internet. É possível encontrar cursos de Modelagem de Banco de dados, Introdução à Segurança da Informação e Tecnologia de Segurança na Internet, Fundamento de Computação e Protocolos TCP/IP, Fundamentos de Virtualização e Computação em nuvem, entre outros.

A Escola de Comunicações ministra 9 (nove) cursos regularmente, entre eles, pode-se destacar o Curso De Gestão De Sistemas Táticos De Comando e Controle, Curso de Operador de Tecnologia Da Informação e Comunicação, Curso de Operador de Tecnologia da Informação E Comunicação, Curso De Proteção Cibernética, que possuem um foco maior em redes de tecnologia da informação.

Quando se observa a rede de tecnologia da informação do Exército Brasileiro e sua estrutura, percebe-se que ela possui uma base grande em software livre. Isso se deve em virtude da Portaria nº 011-DCT, de 29 de março de 2010, que aprova o Plano de Migração para Software Livre no Exército Brasileiro, versão 2010. Essa portaria tem por finalidade definir as atividades a serem realizadas para a transição dos *softwares* e das infraestruturas de tecnologia de informação do Exército Brasileiro para a plataforma de *software* livre. Cabe ressaltar que isso contribui para promover a independência tecnológica e de fornecedor, além de racionalizar os recursos em virtude de os *softwares* livres não necessitarem da compra de licenças. Além disso, é de extrema importância possuir o código fonte das soluções de TI aplicadas na rede do exército por questões de segurança tecnológica, pois quando se utiliza softwares gratuitos ou proprietários, sem ter acesso ao código fonte, não se sabe claramente como as informações estão sendo tratadas.

O Exército Brasileiro está empenhado na defesa do ciberespaço brasileiro. Com isso, a portaria nº 3,781/GM-MD, de 17 de novembro 2020, criou o Sistema Militar

de Defesa Cibernética (SMDC), tendo como órgão responsável o Comando de Defesa Cibernética (Com D Ciber). O domínio cibernético está diretamente relacionado com os Sistemas de Tecnologia da Informação e Comunicação (TIC). O ciberespaço não possui limites e fronteiras físicas, mas o seu poder de influência pode ser observado nas dimensões física e virtual. É um ambiente complexo, onde a segurança é fundamental para garantir a integridade e confidencialidade das informações. Isso tornou o domínio da defesa cibernética extremamente importante para garantir a segurança de um país, pois os danos causados no ciberespaço transcendem o mundo virtual e causam graves consequências no mundo físico.

> A partir do estabelecimento do setor cibernético, decorrente da aprovação da Estratégia Nacional de Defesa, em 2008, dois campos distintos passaram a ser reconhecidos: a segurança cibernética, a cargo da Presidência da República (PR), e a defesa cibernética, a cargo do MD, por meio das FA. (BRASIL, 2017, p.14)

A Guerra Cibernética ocorre em um campo de batalha baseado em TIC, quanto mais um oponente possui os seus sistemas baseados em redes de tecnologia da informação, maiores são os estragos de um ataque cibernético bem-sucedido.

> GUERRA CIBERNÉTICA – corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar capacidades de C2 AO adversário, explorá-las, corrompê-las, degradá-las ou destruí-las, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de TIC para desestabilizar ou tirar proveito dos sistemas de informação do oponente e defender os próprios Sist Info. Abrange, essencialmente, as ações cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação às TIC. (BRASIL, 2017, p.18)

As atividades da guerra cibernética são divididas em ataque cibernético, exploração cibernética e proteção cibernética.

O ataque cibernético é uma atividade maliciosa que tem como objetivo interromper, negar o uso, degradar, corromper ou destruir sistemas computacionais ou informações armazenadas em dispositivos e redes computacionais e de comunicações de interesse. Esses ataques podem ser realizados por indivíduos ou grupos com motivações variadas, incluindo ganho financeiro, espionagem, ativismo político ou simplesmente para causar danos ou adquirir algum reconhecimento global individualmente ou para grupo que representa. (BRASIL, 2017)

A exploração cibernética é uma atividade que visa à obtenção de informações em sistemas de informação de interesse, a fim de coletar o máximo de informações possíveis e obter a consciência situacional do ambiente cibernético. Isso pode incluir a coleta de informações sobre vulnerabilidades de segurança, configurações de rede, dados pessoais e outras informações sensíveis. Os atores mal-intencionados podem usar essas informações para realizar ataques cibernéticos mais sofisticados ou para fins de espionagem. (BRASIL, 2017)

A proteção cibernética possui como objetivo neutralizar o ataque e a exploração cibernética oponentes contra os dispositivos computacionais, as redes de computadores e de comunicações amigos. É uma atividade de caráter permanente, ou seja, não é preciso sofre um ataque para que ela ocorra. Tais ações visam garantir a integridade e a segurança da rede e, muitas vezes, é realizada na forma de defesa em profundidade que consiste em introduzir múltiplas camadas de proteção a fim de reduzir a probabilidade de comprometimento dos sistemas, caso haja alguma falha em uma cama, o invasor não conseguirá acesso pleno a rede comprometida. (BRASIL, 2017)

É importante que os militares tomem medidas para proteger seus sistemas e informações contra esses tipos de ameaças. Isso pode incluir a implementação de medidas de segurança cibernética, como firewalls, software antivírus, treinamento de conscientização de segurança para usuários e o monitoramento contínuo de suas redes e sistemas. Além disso, é importante manter os sistemas atualizados com as últimas correções de segurança e seguir as melhores práticas de segurança cibernética, realizando medidas proativas mediantes as ameaças cibernéticas. Isso pode ser realizado ao realizar avaliações regulares de segurança e a implementação de uma política de procedimentos para gerenciar o risco cibernético, ajudando a minimizar o risco de um ataque cibernético bem-sucedido.

Para que essas medidas sejam implementadas, há a necessidade de um indivíduo com o domínio sobre o conhecimento de TI, onde figura o militar da Arma de Comunicações.

As atividades de guerra cibernética envolvem uma série de tarefas, muitas delas, exigem um conhecimento profundo de TI para serem realizadas e, quanto mais qualificado for um militar dentro do domínio das redes de computadores, maior será a probabilidade de sucesso ao realizar tais atividades

De acordo com o Manual de Campanha EB70-MC-10.232 Guerra Cibernética (2017, p.30-31) pode-se destacar as atividades e tarefas da guerra cibernética:

Atividade	Tarefa
Proteção Cibernética	**Gestão de Riscos** Gerenciar as relações entre ativos de informação, patrimônio digital, ameaças, vulnerabilidades, impactos, probabilidade de ocorrência de incidentes de segurança da informação e riscos. Estabelece o nível de alerta cibernético correspondente e executa o tratamento, a comunicação e a monitoração contínua desses riscos.
	Gestão de Riscos Gerenciar as relações entre ativos de informação, patrimônio digital, ameaças, vulnerabilidades, impactos, probabilidade de ocorrência de incidentes de segurança da informação e riscos. Estabelece o nível de alerta cibernético correspondente e executa o tratamento, a comunicação e a monitoração contínua desses riscos.
	Consciência Situacional Monitorar sistematicamente o espaço cibernético de interesse do EB no tocante à possibilidade de concretização de ameaça, de modo a estar em condições de decidir e aplicar as ações requeridas conforme as condições do espaço cibernético.
	Defesa Ativa Detectar, identificar, avaliar e neutralizar vulnerabilidades nas redes de computadores e sistemas de informação em uso pelo EB, antes que elas sejam exploradas. Mediante ordem, desencadear ações ofensivas contra a fonte da ameaça, mesmo que localizada fora do espaço cibernético defendido.
	Pronta Resposta Reagir prontamente às ameaças identificadas, observando os diferentes níveis de alerta cibernético (grau de risco).
	Forense Digital Coletar e examinar evidências digitais em redes e sistemas de informação de interesse do EB.
	Teste de Artefatos Cibernéticos Testar, simular, analisar, avaliar e homologar artefatos e sistemas cibernéticos.
	Conformidade de SIC Verificar a observância de aspectos legais, normativos e procedimentais de SIC no âmbito do SGCEx.
	Gestão de Incidentes de Redes Coordenar o tratamento de incidentes nas redes de interesse, acompanhar a solução e acionar procedimentos.
	Controle de Acesso

	Permitir que os administradores e gerentes determinem o que os indivíduos podem acessar, de acordo com suas credenciais de segurança, após a autorização, a autenticação, o controle e a monitoração dessas atividades.
Proteção Cibernética	**Proteção das comunicações** Examinar os sistemas de comunicações internos, externos, públicos e privados; estruturas de rede; dispositivos; protocolos; acesso remoto e administração.
	Emprego de Criptografia Empregar técnicas, abordagens e tecnologias de criptografia.
	Implementação de controles de segurança Controlar atividades de pessoal e procedimentos de segurança, na utilização dos sistemas necessários às atividades na área cibernética.
	Segurança Física Autorizar a entrada e estabelecer os procedimentos de segurança do ambiente operativo, a fim de proteger instalações, equipamentos, dados, mídias e pessoal contra ameaças físicas aos ativos de informação.
	Gestão da Continuidade da Missão e Recuperação de Desastres Preservar as atividades operativas por ocasião da ocorrência de interrupções ou de catástrofes.
Ataque Cibernético	**Reconhecimento** Investigar em fontes abertas para obter informações sobre o alvo.
	Escaneamento (*Scanning*) Encontrar falhas na proteção cibernética do alvo.
	Exploração da Vulnerabilidade Realizar ações como: obter acesso, degradar uma aplicação ou negar acesso para outros usuários.
	Manutenção do acesso Manipular *software* instalado no sistema alvo com objetivo de disponibilizar um *backdoor* para acesso futuro.
	Cobertura de rastros Ocultar as ações realizadas no sistema alvo com objetivo de impedir ou dificultar que usuários e/ou administradores identifiquem as ações de um atacante.
Exploração Cibernética	**Inteligência Cibernética** Realizar ações de busca e de coleta de dados no espaço cibernético, para a produção do conhecimento de Inteligência.

Quadro 1 – Atividades e Tarefas de Guerra Cibernética
Fonte: Brasil (2017)

Dada a devida importância da necessidade do conhecimento de redes de computadores e procurando mais a “ponta da linha”, usuário final, Chaves (2022)

aplicou um questionário em diversas OM de comunicações do Brasil sobre a formação do cabo e do soldado de comunicações, mais precisamente, sobre a parte de redes de computadores. Em seu questionário, conforme pergunta número 3, é possível verificar que os entrevistados reconhecem a necessidade e a importância do conhecimento e redes de TI (figura 6) e, outro dado preocupante, conforme pergunta número 5, é que pouco mais da metade dos Cb e Sd, possivelmente, sabem realizar configurações, ajustes ou resoluções de problemas relativos a redes ou pelo menos passam essa impressão para os entrevistados.

3. O Sr acha importante que os Cb/Sd qualificados nas QM 1171,1173 e 1174 (combatente, manutenção e operador de comunicações respectivamente) tenham conhecimento de redes de computadores?

GRÁFICO 6 – Respostas da questão 3
Fonte: Chaves (2022)

4. Você acredita que os Cb e Sd de sua OM têm as capacidades necessárias para cumprir suas atribuições: realizar configurações, ajustes ou resolução de problemas relativos a redes?

GRÁFICO 6 – Respostas da questão 5
Fonte: Chaves (2022)

Na pergunta número 3, os participantes concluíram unanimemente que o conhecimento de redes de computadores é importante para os cabos e soldados da qualificação comunicações.

Na pergunta número 5, é possível verificar que quase 40% dos militares não sabem ou não passam confiança que sabem realizar operações básicas de TI, o que é preocupante tanto com relação a capacidade operacional quando em questão de segurança das redes de TI, pois o usuário é uma das principais portas de entradas para atividades hackers.

Chaves (2022) sugere inclusive a reformulação da formação do Cabo e Soldado da Arma de Comunicações de forma que essa formação aborde de maneira mais eficiente o conhecimento de redes de TI.

2.2.4 **Redes de Tecnologia da Informação nos conflitos e a importância da segurança dos ativos**

As redes de tecnologia da informação estão fortemente ligadas aos conflitos bélicos atuais. Quando observamos o conflito entre a Rússia e a Ucrânia, nunca

esteve tão presente a guerra cibernética, a invasão de sistemas, a atuação de hackers, ataques do tipo DDoS.

Uma rede de TI mal estruturada e com várias brechas de segurança pode ter seus dados comprometidos e os danos podem ser imensuráveis em um conflito, tanto para militares quanto para civis.

> Se a indisponibilidade de internet, os ataques que tiram sistemas do ar e os sequestros de informações sigilosas paralisam empresas e órgãos em tempos de paz, os efeitos são ainda mais devastadores em uma guerra. Principalmente para os civis, que acabam ficando sem informações confiáveis sobre como se proteger ou fugir e ficam incapazes de se comunicar. (IGREJA, 2022)

Suzuki (2022) chama a atenção para as ações cibernéticas que ocorreram na Ucrânia. Em um país que está vivendo um conflito armado, a realização de ataques aos ativos de TI, derrubar redes telefonia e espalhar a desinformação geram choques de efeitos psicológicos na população, pois a ideia de desnortear o adversário é uma das bases das ofensivas hackers.

> O objetivo é criar confusão, é fazer com que as pessoas se sintam perdidas. Disparar em massa desinformação é parte de uma guerra psicológica, para minimizar as chances de os ucranianos terem uma reação, afirma Luca Belli. Foi o que aconteceu nos últimos dias. Foi difundido que o presidente ucraniano tinha fugido do país e depois ele postou vídeos mostrando que isso não era verdade. Imagine o efeito de espalhar que o próprio presidente já abandonou o país. O efeito psicológico é devastador nas pessoas.

Dada a magnitude que tomou o conflito entre a Ucrânia e a Rússia, países como Estados Unidos começaram a contratar empresas para “blindar” as suas redes de TI. Conforme Tidy (2022) publicou em sua reportagem “O presidente dos Estados Unidos, Joe Biden, convocou empresas e organizações nos EUA a "trancar suas portas digitais". A Casa Branca reconhece a que a Rússia é uma superpotência cibernética com hacker altamente capacitados e com capacidade de ataques disruptivos e potencialmente destrutivos, tanto no meio físico quanto digital, e teme sofrer ataques cibernéticos em virtude das sanções que não só os EUA, mas todo o ocidente tem imposto sobre a Rússia.

De acordo com Tidy (2022) os três ataques que os especialistas mais temem são o “BlackEnergy”, NotPetya e o ataque ao fornecimento de combustível.

> Um ataque cibernético chamado **"BlackEnergy"**, que causou um apagão de curta duração que afetou 80 mil pessoas no oeste do país. Quase um ano depois, outro ataque cibernético, que ficou conhecido como "Industroyer", bloqueou o fornecimento de energia elétrica em cerca de um quinto de Kiev, a capital ucraniana, por cerca de uma hora.
> O **NotPetya** é considerado o ataque cibernético que mais prejuízos financeiros causou na história. O software com poder de destruição foi colocado em uma atualização de um programa de computador bastante usado para contabilidade na Ucrânia, mas se espalhou pelo mundo, devastando sistemas de computador de milhares de empresas e causando aproximadamente US$ 10 bilhões em danos.
> Em maio de 2021, vários Estados dos EUA adotaram esquemas de emergência depois que hackers conseguiram **bloquear as operações de um oleoduto** importante. O oleoduto transporta 45% do suprimento de diesel, gasolina e combustível de aviação da Costa Leste dos Estados Unidos. A empresa afetada admitiu pagar aos criminosos US$ 4,4 milhões (mais de R$ 21 milhões) em Bitcoin com rastreabilidade dificultada para retomar o funcionamento dos sistemas. (grifo nosso)

O profissional de TI é responsável por uma rede que pode possuir inúmeros informações de grande relevância, tanto para ambientes de guerra e não guerra. Quando uma rede é comprometida, ela pode vazar informações sigilosas, ter seu banco de dados com informações pessoais roubados ou inutilizados e projetos em desenvolvimentos perdidos. TRINDADE (2019), destaca 4 grandes ataques cibernéticos da história:

> Stuxnet (2010)
> Ataque conjunto ligado a EUA e Israel que resultou na falha de centrífugas em uma instalação de enriquecimento de materiais nucleares do Irã, sem que operadores notassem o problema nos sistemas de controle industrial do local.
> NotPetya (2017)
> Ferramenta chamada NotPetya criptografava os dados de computadores-alvo e inutilizava-os. Ligado à Rússia, malware foi disseminado por um software de declaração de impostos na Ucrânia.
> Wannacry (2017)
> Malware criado para criptografar dados de redes que usassem Windows. O objetivo era receber dinheiro de "resgate", com a entrega da chave para que redes voltassem ao normal. Foi ligado à Coreia do Norte.
> Shamoon (2012)
> Malware apagou dados de 35 mil computadores da empresa petrolífera Saudi Aramco, da Arábia Saudita. Senhas foram roubadas, dados apagados e PCs não reiniciavam. Ataque tem ligações ao Irã.

A segurança de uma rede de TI começa pelo profissional que a utiliza. Os militares da Arma de Comunicações, envolvidos constantemente na montagem de centro de operações em ambiente de operação, necessitam de um mínimo de conhecimento de redes de TI para garantir a segurança dos dados que serão empregados na operação. O comunicante tem que saber a importância do uso de uma VPN, de um firewall de proteção, de um antivírus, da necessidade de manter os

sistemas atualizados, da divisão de redes, para que ele possa garantir a integridade e a segurança das atividades.

Quando se fala em combate moderno, a tecnologia torna-se um fator importante no processo decisório. Pode-se citar o termo “operações capacitadas por rede”, que é explicado por Burken (2013):

> Significa o uso de tecnologias de rede e recursos da tecnologia da informação para facilitar a cooperação e o compartilhamento de dados. Isso pode levar a um acúmulo de ambientes multinacionais complexos e *ad hoc*, referidos como capacidades facilitadas por redes ou operações capacitadas por redes. As capacidades facilitadas por redes oferecem o potencial de aumentar os efeitos militares por meio do uso aperfeiçoado de sistemas de tecnologia da informação.

A tecnologia se tornou um multiplicador de poder ao mesmo tempo que tornou os combates mais complexos.

> Os avanços no profissionalismo parecem estar positivamente correlacionados com os avanços da tecnologia e a crescente especialização que eles exigem. À medida que a tecnologia melhora, a luta de guerra se torna mais complexa. Com cada interação de tecnologia – de catapultas a artilharia, cavalaria montada a cavalo a veículos blindados, velas a vapor, balões de ar quente a voo de asa fixa – os militares desenvolveram novas competências essenciais. Impulsionadas pela tecnologia, essas novas competências essenciais exigiram um desenvolvimento igual da compreensão técnica dentro da força profissional que as coloca. (FINNEY, 2018, tradução nossa)

A literatura tem nos mostrado a importância dos equipamentos de tecnologia da informação e comunicação e que muitos países têm investido pesado no desenvolvimento de avançados meios de comunicações, cibernéticas e guerra eletrônica.

A era da informação tem mostrado que cada vez mais a tecnologia está interligando o mundo e a velocidade da informação está cada vez maior, sendo preciso apenas alguns segundos para realizar grandes decisões e grandes estragos. É nesse ambiente invisível e inteiramente digital que ocorre a Guerra Cibernética em que sistemas de computadores de vários países “lutam” entre si com o objetivo de adquirir superioridade informacional ou causar o maior dano possível ao sistema de informação do oponente.

O ambiente virtual criado pelas redes de tecnologia da informação tem abrangência global, ou seja, pode ser atacado que qualquer parte do mundo, basta

apenas estar conectado. Nesse contexto, pode ser criado um campo de batalha de interesses e nele atua a guerra cibernética e cibercriminosos, diferenciados, geralmente, pela motivação, sendo o primeiro motivado por questões políticas e o segundo por questões, principalmente, financeiras.

De acordo com a Compugraf, em 2019, o Brasil era o 4º no ranking de ataques cibernéticos, perdendo penas para os EUA, China e Rússia. Dados da empresa Kaspersky, apontam que só no primeiro trimestre de 2020, as tentativas de golpes de *ransomware* no Brasil aumentaram em 350%.

No ano de 2021, o Brasil sofreu 5 ataques cibernéticos que despertaram um alerta para a questão da segurança dos meios de TI. Empresas como Lojas Renner, CVC, Porto Seguro, Atento e Serasa Experian tiveram seus bancos de dados atacados e seus clientes e usuários expostos ou seus sistemas inoperantes. Mario Toews, que é DPO, especialista em Segurança da Informação e sócio fundador da Datalege Consultoria Empresarial, fez a seguinte observação:

> A internet está cada vez mais popularizada e se tornou essencial na vida das pessoas. Mas as ferramentas de segurança ainda não são usadas adequadamente, nem pelos consumidores e nem mesmo pelas empresas

O site CNN BRASIL coloca o Brasil como o segundo da América Latina a receber mais ataques em 2022, ficando atrás apenas do México, que teve 85 bilhões de tentativas e, seguindo lista aparecem países como a Colômbia, com 6,3 bilhões de ataques e, em quarto lugar, o Peru, com 5,2 bilhões.

2.2.4 **A Formação do militar da Arma de Comunicações no Exército Brasileiro**

No Exército Brasileiro, o conhecimento de redes de Tecnologia da Informação a ser ministrado na formação do militar de comunicações, assim como toda a parte de informática, está previsto nos Planos de Disciplina (PLADIS) e nos Programas Padrões de Instrução dos militares da Arma de Comunicações.

Começando pelos soldados e cabos da qualificação Comunicações, que possuem sua qualificação baseada no EB70-PP-11.204 Programa-Padrão de Instrução de Qualificação do Cabo e Soldado de Comunicações, pode-se observar

que a carga horária prevista de redes de TI corresponde a 17 (dezessete) horas da matéria peculiar de Informática. Nessa disciplina estão previstas tarefas como: apresentação dos componentes do microcomputador, preparar um microcomputador para o funcionamento, descrever as finalidades e o funcionamento do sistema operacional e dos aplicativos, instalar e configurar uma impressora, definir as principais características de uma rede de computadores e executar a manutenção de 1º Escalão.

A formação dos 3º sargentos temporários e dos 3º sargentos de carreira são diferentes. O 3º Sargento de carreira é formado na Escola de Sargentos das Armas por meio de um PLADIS, enquanto o 3º sargento temporário é formado nas unidades de corpo de tropa por meio de programas padrões de instrução de formação.

Os cabos e os soldados de comunicações podem realizar o Curso de Formação de Sargentos Temporários (CFST) e serem promovidos a graduação de 3º sargento de comunicações. O 3º sargento temporário tem sua formação baseada no EB70-PP-11.022 Programa-Padrão de Instrução de Formação do 3º Sargento Temporário de Comunicações, nele pode-se observar que o militar possui previsto em sua formação 70 (setenta) horas da matéria peculiar Informática e Redes de Computadores. Nessa matéria são previstas instruções para: conhecer as principais ferramentas de internet, preparar o microcomputador para funcionamento, preparar o microcomputador para funcionamento, descrever a finalidade o funcionamento do sistema operacional e dos aplicativos, descrever a finalidade e o funcionamento do sistema operacional e dos aplicativos, instalar, configurar e compartilhar uma impressora na rede, definir as principais características de uma rede de computadores, definir as principais características de uma rede de computadores, confeccionar um patch panel, preparar e colocar em funcionamento os serviços de uma rede de computadores, preparar um link rádio e definir as características dos seus principais componentes, descrever e configura uma VPN, instalar e configurar um equipamento VOIP, descrever, instalar e configurar softwares de Comando e Controle, descrever, instalar e configurar softwares de Comando e Controle, executar a manutenção de 1º Escalão, conhecer o sistema de radiofrequências utilizadas no Brasil.

O PLADIS do 3º sargento de carreira possui a disciplina Cibernética com uma carga horária de 106 (cento e seis) horas. Ela é dividida em 4 (quatro) unidades didáticas (UD):

- UD I Introdução a Redes, com as matérias: a. LAN, WAN e a Internet, b. Configuração de um sistema operacional de rede, c. Protocolos e comunicações de rede, d. Acesso à rede, e. Ethernet, f. Camada de rede, g. Camada de transporte, h. endereçamento IP, i. Divisão de redes IP em sub-redes e j. Camada de aplicação.

- UD II Enlaces de Redes, com as matérias: a. Introdução, b. Configuração de *Access Point*, c. Configuração de aparelhos da Ubiquiti.

- UD III GNU/Linux, com as matérias: a. Discos e partições de disco, b. Sistemas de arquivos, c. Estrutura de diretórios, d. Comandos essenciais, e. *Advanced Package Tool* (APT), f. Comandos de visualização de conteúdo de arquivos, g. Comandos de gerenciamento de redes, h. Comandos de gerenciamento de contas, i. Comandos de gerenciamento de memória e processamento, h. Comandos de gerenciamento de contas, i. Comandos de gerenciamento de memória e processamento, j. Comandos para gerenciamento de permissões, k. SSH, e l. Instalação de Distribuição Linux.

- UD IV Servidores Linux, com as matérias: a. Implementação de um Firewall utilizando a ferramenta opensource pfSense, b. *Domain Name Service* DNS (BIND9), c. Servidor de e-mail (Zimbra), d. Servidor LAMP (Apache, PHP, MySQL e PHPMyAdmin), e. VOIP (FreePBX), f. Servidor FTP (SME SERVER) e g. Virtualização.

A formação do oficial de comunicações de carreira do Exército Brasileiro ocorre na Academia Militar das Agulhas Negras (AMAN). Nesse estabelecimento de ensino o militar passa por 4 (quatro) de formação, sendo apenas no segundo ano que o militar escolhe a sua Arma/Quadro/Serviço. Dessa forma, realiza apenas 3 anos de instrução peculiar dentro de sua escolha.

O PLADIS do 2º ano de comunicações da AMAN possui a disciplina Cibernética III com uma carga horária de 152 (cento e cinquenta e duas) horas. Ela é dividida em 3 (três) unidades didáticas (UD):

- UD I Cisco Certified Network Associate I (CCNA I), com as matérias: a. O impacto das redes de computadores em nossas vidas, b. Características da arquitetura de rede, c. Estrutura de rede modelo OSI e TCP/IP, d. IPV4, e. Endereçamento IP, redes e sub-redes, f. *Unicast*, *multicast* e *Broadcast* e g. Ferramenta de emulação/simulação de rede.

- UD II Cisco Certified Network Associate II (CCNA II), com as matérias: a. Funcionamento de switches, b. Gerenciamento de *switches*, c. Tabela MAC, d.

Gerenciamento avançado de *switch,* e. Funcionamento de roteadores, f. Gerenciamento de roteadores, g. Tabela de roteamento, h. LAN, WAN e MAN, i. Roteamento estático, j. Roteamento dinâmico (RIP/OSPF) e k. Wrapping-Up,

- UD III Infraestrutura de Rede, com a matéria: a. Infraestrutura de rede.

O PLADIS do 3º ano de comunicações da AMAN possui a disciplina Cibernética IV com uma carga horária de 80 (oitenta) horas. Ela é dividida em 4 (quatro) unidades didáticas (UD):

- UD I Gerenciamento de Máquinas Virtuais, com a matéria: a. Máquinas virtuais.

- UD II Administração de Sistemas Linux, com as matérias: a. Instalação do Sistema Linux, b. Sistema de Arquivos do Linux, c. Editores de Texto, d. Configuração de Rede, e. Gerenciamento de Usuários e Grupos, f. Gerenciamento de *Backup* e g. Registro de Eventos.

- UD III Serviços de rede, com as matérias: a. Serviço *Web*, b. *Dynamic Host Configuration Protocol* (DHCP), c. *Domain Name System* (DNS), d. *File Transfer Protocol* (FTP) e e. *Network Time Protocol* (NTP).

- UD IV: *Firewall, com a matéria: a. Firewall de Rede.*

O PLADIS do 4º ano de comunicações e último ano de formação da AMAN possui a disciplina Cibernética V com uma carga horária de 77 (setenta e sete) horas. Ela é dividida em 4 (quatro) unidades didáticas (UD):

- UD I Guerra Cibernética (G Ciber), com a matéria: a. G Ciber.

- UD II *Proxy*, com a matéria: a. Servidor *Proxy*.

- UD III: *Hardening*, com a matéria: a. *Hardening*, b. Acesso ao Sistema Operacional GNU/Linux, c. Particionamento, d. Quotas de disco e e. Lista de Controle de Acesso.

- UD IV *CyberSecurity Essentials*, com as matérias: a. *Cyber Kill Chain*, b. *Malwares* e Ataques Cibernéticos, c. Engenharia Social e d. Controle de Acesso.

3. METODOLOGIA

Os procedimentos metodológicos que foram desenvolvidos consistiram em leitura para o aprofundamento do conhecimento sobre redes de tecnologia da informação e coleta de informações sobre a aplicação desse conhecimento em operações militares e não militares e, por fim, discutiu-se os resultados encontrados.

No decorrer da pesquisa foram realizados os seguintes procedimentos: pesquisa bibliográfica relacionada à temática de redes de tecnologia da informação, coleta de dados por meio de livros, artigos científicos, revistas, jornais, trabalhos de conclusão de curso, redes eletrônicas, manuais doutrinários e outros conteúdos de acesso ao público geral, análise dos dados e verificação dos resultados. Inicialmente, a pesquisa se concentrou em leitura e fichamento de trabalhos anteriores e de livros, para desenvolver os conceitos necessários para o estudo.

A análise dos dados procurou levantar a importância do conhecimento de redes de TI para os militares da Arma de Comunicações e a aplicabilidade desse conhecimento para eles.

Os resultados foram associados a importância do conhecimento de redes de TI para a vida profissional do militar. Assim, pretendeu-se alcançar os objetivos e levantar os principais reflexos que podem trazer para o exercício da função.

Quanto à forma de abordagem do problema, utilizou-se principalmente os conceitos de pesquisa qualitativa**,** apresentando o resultado através de análises dos conteúdos encontrado.

Quanto ao objetivo geral foi empregada a modalidade exploratória, a fim de realizar uma maior familiarização com o tema, materializada pelas pesquisas realizadas.

3.1 OBJETO FORMAL DE ESTUDO

O presente trabalho teve como objetivo apresentar a importância do conhecimento de redes de TI para os militares da Arma de Comunicações e a aplicabilidade desse conhecimento para os comunicantes na atualidade.

3.2 AMOSTRA

A amostra para o desenvolvimento da pesquisa limitou-se a pesquisa bibliográfica e documental para conteúdos publicados preferencialmente nos últimos 10 (dez) anos, sendo observados de forma criteriosa, os conteúdos encontrados que possuíam data de publicação anterior ao ano de 2013, tendo em vista os saltos tecnológicos ocorridos nos últimos anos.

3.3 DELINEAMENTO DA PESQUISA

O delineamento da pesquisa consistiu em pesquisa bibliográfica e documental, realizada por meio de livros, artigos científicos, revistas, jornais, trabalhos de conclusão de curso, redes eletrônicas, manuais doutrinários e outros conteúdos de acesso ao público geral, realizando uma leitura analítica dos conteúdos para a formulação da conclusão.

3.3.1 **Procedimentos para revisão da literatura**

Para o levantamento da bibliografia e das outras fontes de consulta, para serem utilizadas no trabalho, foram realizados os seguintes procedimentos:

a. Fontes de busca

- Trabalhos de Conclusão de Curso, disponibilizados na Biblioteca Digital do Exército (BDEx).
- Manuais doutrinários do Exército.
- Artigos.
- Livros sobre TI.
- Revistas digitais.
- Artigos Científicos.

- Reportagens na Internet.
- Planos de disciplinas.

b. Estratégia de busca para as bases de dados eletrônicas

Para a realização da busca dos conteúdos, foram utilizados sites de buscas na Internet como Google, para as buscas mais amplas, e, para buscas mais focadas em trabalhos realizados sobre o assunto, sites como o Google Acadêmico, Biblioteca Digital do Exército e EB Revistas. A fim otimizar a busca, utilizou-se os seguintes termos descritores para conseguir resultados melhores nas pesquisas: redes de tecnologia da informação, tecnologia da informação, tecnologia da informação Exército.

3.3.2 **Procedimentos Metodológicos**

Sobre as fontes encontradas para o trabalho, procurou-se seguir os seguintes critérios:

a. Critérios de inclusão:

- Estudos em português e inglês, sobre redes de tecnologia da informação.
- Estudos envolvendo redes de computadores.
- Estudos que mostrem a aplicabilidade do conhecimento de redes de TI e suas vantagens no exercício da atividade da Arma de Comunicações.
- Estudos que tragam em seu conteúdo os benefícios do desenvolvimento e estruturação de uma rede de TI.
- Estudos sobre tecnologia de informação envolvendo atividades militares e não militares ou que possam ser empregados em benefício delas.

b. Critérios de exclusão:

- Estudos que não envolvam redes de TI.
- Estudos cujo foco seja TI sem aplicabilidade para o meio militar.
- Estudos que abordem benefícios que não possam ser aplicados pelos militares da Arma de Comunicações.

3.3.3 **Instrumentos**

O instrumento para coleta de dados será a análise de materiais e documentos de conteúdos já existentes como livros, manuais, artigos, revistas e outros documentos de acesso ao público em geral.

3.3.4 **Análise dos Dados**

Para uma melhor compreensão do objeto de estudo, buscou-se bibliografias sobre Tecnologia da Informação (TI) e redes de TI, para dar uma melhor definição para o objeto de estudo. Após isso, analisou-se o conteúdo encontrado de forma a realizar uma seleção e focalização naquilo que é de interesse deste estudo, descartando o que não seja de interesse ou que não possua relevância para o trabalho. Por fim, compreender o significado das informações de forma a realizar a conclusão do trabalho.

4. RESULTADOS

A bibliografia utilizada como fonte de consulta para este trabalho possui várias ideias força que contribuíram para fundamentar a conclusão deste estudo. Dessa forma, para melhor organizar essas ideias, procurou-se organizá-las de acordo com temas ou tópicos relevantes. Além disso, as informações apresentadas na bibliografia foram avaliadas de maneira crítica, considerando a relevância, confiabilidade e precisão. Ao organizar e avaliar as informações e ideias da bibliografia, foi possível agrupá-las, para melhor compreensão, da seguinte forma:

Fonte	Síntese do conteúdo	Contribuição para o trabalho
Morton Grosso Mendes Algar Telecom	Trazem algumas definições sobre Tecnologia da Informação e Comunicação.	Ajudam a entender melhor o que é Tecnologia da Informação e Comunicação.
Zabbix	*Software* de gerenciamento e monitoração de redes e outras ferramentas.	Ferramentas que podem ser utilizadas pelos comunicantes em benefício da atividade militar.
PROXMOX	*Software* de virtualização para executar máquinas virtuais e contêineres e outras ferramentas.	
OpenMeetings	*Software* para realização de apresentações/videoconferências com várias ferramentas.	
Remmina	*Software* para gerenciamento/suporte remoto/acesso remoto para profissionais de TI.	
Zimbra Collaboration	*Software* que oferece funcionalidades como e-mail, bate-papo e videoconferência	
Chaves	Importância do conhecimento de TI para Cabos e Soldados da qualificação militar Comunicações do Exército Brasileiro.	Destaca a importância do conhecimento de redes de computadores para cabos e soldados de comunicações e seus óbices na formação.
Portaria nº 193 do Estado Maior do Exército (EME), de 22 de	Aprova a Diretriz para a Implantação do Projeto Sistema Integrado de Monitoramento de Fronteiras (SISFRON).	Surge junto com o projeto o Módulo de Telemática Operacional, uma Viatura de Comando e Controle que demanda grande

dezembro de 2010		conhecimento de TI para sua operação
Escola de Comunicações	Habilitar militares a exercerem as atribuições do cargo a que se destinam, especialmente na área de Comunicações no Exército Brasileiro	Estabelecimento de ensino voltado para especializar militares, principalmente de comunicações, em conhecimento que envolvem redes de TI e outros.
Manual de Campanha EB20-MC-10.205 Comando e Controle	Apresentar a função de combate Comando e Controle (C2), apresentando os conceitos básicos e as concepções operacionais que caracterizam o C2 no âmbito do Exército Brasileiro (EB)	Destaca a quantidade de sistemas que empregam o conhecimento de redes de TI dentro do EB.
Regulamento Interno e dos Serviços Gerais - R-1 (RISG)	Regulamento Interno do Exército que define as atribuições das diversas funções desempenhadas dentro do EB.	Destaca a função do Oficial de Informática que, muitas vezes, é desempenhada por um militar da Arma de Comunicações e a aplicabilidade do conhecimento de redes de TI no desempenho de sua função.
Portaria nº 011-DCT, de 29 de março de 2010	Aprova o Plano de Migração para Software Livre no Exército Brasileiro, versão 2010.	Explica o motivo da ênfase da utilização de *softwares* livres no Exército Brasileiro.
Portaria nº 3,781/GM-MD, de 17 de novembro 2020	Cria o Sistema Militar de Defesa Cibernética (SMDC)	Demonstra a importância do domínio cibernético e como ele está associado ao Sistema de Tecnologia da Informação e Comunicação (TIC)
Manual de Campanha EB70-MC-10.232 Guerra Cibernética	Estabelecer os conceitos e concepções da Doutrina de Guerra Cibernética do Exército Brasileiro (EB)	Disserta sobre Guerra Cibernética, as atividades realizadas nesse domínio digital como ataque, exploração e proteção, e destaque como essa atividade está intimamente ligada as redes de tecnologia da informação
Trindade	Traz 4 (quatro) grandes casos de ataques cibernéticos.	Demonstra os danos que podem ocorrer em virtude de um ataque cibernético por meio de uma rede de tecnologia da informação.

Burken	Aborda o combate moderno e coloca a tecnologia como um fator importante no processo decisório.	Destaca o uso de tecnologias de rede e recursos da tecnologia da informação para facilitar a cooperação e o compartilhamento de dados, ajudando nos processos decisórios.
Suzuki Compugraf CNN BRASIL Tidy	Dados sobre ataques cibernéticos.	Mostram o quão impactante pode ser um ataque cibernético em uma empresa/país
EB70-PP-11.204 Programa-Padrão de Instrução de Qualificação do Cabo e Soldado de Comunicações EB70-PP-11.022 Programa-Padrão de Instrução de Formação do 3º Sargento Temporário de Comunicações	Define as instruções que são ministradas na formação dos militares temporários	Define o conhecimento de redes de TI, TIC e cibernética que o militar deve possuir ao final de sua formação.
Plano de Disciplina (PLADIS) do 3º sargento de carreira Plano de Disciplina (PLADIS) do 2º, 3º e 4º ano de formação do oficial de comunicações da AMAN	Define as disciplinas que são ministradas durante a formação dos militares de carreira.	Define o conhecimento de redes de TI, TIC e cibernética que o militar deve possuir ao final de sua formação.

QUADRO 2 – Resumo de ideias força
Fonte: O autor

A primeira coluna, denominada “Coluna Fonte”, indica a origem da ideia central apresentada. Essa origem pode ser um autor, uma empresa ou instituição, ou mesmo um documento específico. A segunda coluna, chamada de “Coluna Síntese”, apresenta a ideia central ou o assunto abordado no trabalho ou documento que é relevante para este estudo. Por fim, a terceira coluna, intitulada “Coluna Contribuição

para o Trabalho”, descreve como o assunto abordado na coluna anterior contribui para os resultados deste estudo.

5. DISCUSSÃO DOS RESULTADOS

Após analisados os dados bibliográficos coletados, procurou-se definir se o conhecimento de redes de Tecnologia da Informação (TI) para os militares da Arma de Comunicações é relevante ou não. Para isso, demonstrou-se, por meio dos dados bibliográficos, as possíveis contribuições que o militar de comunicações oferece ao possuir um conhecimento desenvolvido e atualizado de redes de TI e como isso influencia no seu desempenho profissional. Dessa forma, procurou-se destacar a aplicabilidade desse conhecimento para o comunicante e quais benefícios e reflexos que isso pode trazer para o exercício de suas funções no Exército Brasileiro.

Como foi observado, a área de rede de tecnologia da informação é muito vasta e cheia de ferramentas que podem contribuir para o cumprimento das atividades militares e administrativas. O militar da Arma de Comunicações pode ganhar muitos benefícios no desempenho de sua função profissional se possuir um conhecimento desenvolvido redes de tecnologia da informação. O conhecimento de TI tornou-se essencial para o comunicante e saber utilizar as ferramentas que estão à disposição de forma segura e eficiente mais ainda. Foi possível observar ferramentas como Zabbix, PROMOX, OpenMeetings, Remmina e Zimbra, podem ser empregadas pelos militares da Arma do Comando em benefício do Comando e Controle e da vida administrativa de suas organizações militares. Essas ferramentas, que são de código aberto, não gerando custos de licença e estão de acordo com a portaria de migração para software livre, podendo serem empregadas para benefício do Exército Brasileiro. Porém, cabe destacar que são ferramentas que, para serem empregadas de forma eficiente e segura, demandam do profissional que as instala e gerencia conhecimento da área de redes de tecnologia da informação, pois da mesma forma que elas podem ser uma aliada do Comando e Controle, quando mal configuradas, podem ser a porta entrada para usuários mal-intencionados.

O Exército Brasileiro, por meio da Escola de Comunicações, oferece várias capacitações para os militares não só da Arma de Comunicações como também para as outras armas, quadros e serviços, demonstrando a importância que o conhecimento de redes de tecnologia da informação adquiriu. É possível perceber que esse conhecimento está direcionado para a Arma de Comunicações em virtude do perfil da Arma, tanto que os cursos são ministrados na Escola de Comunicações.

Isso mostra a importância da capacitação dos comunicantes em saber utilizar a tecnologia que está a sua disposição da maneira mais eficiente e segura possível. A falta de conhecimento pode dificultar o uso das ferramentas que estão disponíveis e pode levar a deixar recursos valiosos de lado devido a sua complexidade de operação por falta de conhecimento, pois ter uma ferramenta com várias capacidades e não usufruir do máximo de sua potencialidade é deixar recursos ociosos e perder potencial de combate.

> O equipamento de comunicação geralmente é complexo, não é amigável ao operador e normalmente requer treinamento específico para configuração inicial, alterações em tempo real e desempenho de funções básicas. Quando a nova tecnologia é problemática ou muito complexa, ela é rotineiramente deixada de lado, colocada em armazenamento ou não usada em todo o seu potencial. (Blumberg, 2020, tradução nossa).

A importância do conhecimento em redes de TI para os militares da Arma de Comunicações, que é uma arma que apoia a decisão do escalão superior por meio de informações que garantem a consciência situacional, ficou mais evidenciada quando se observa os sistemas de comunicações empregados no EB.

> Os sistemas de TIC permeiam todas as atividades operacionais e de apoio, em todos os níveis de decisão (político, estratégico, operacional e tático), assegurando o fluxo de informações que direciona e sincroniza tais atividades. Desse modo, contribuem para a interoperabilidade entre os diversos componentes das FA empregados nas operações conjuntas e para a obtenção da consciência situacional. (BRASIL, 2015, p. 14)

Da mesma forma, pode-se observar que o conhecimento de redes de TI permeia o domínio da informação que é de extrema importância para o Comando e Controle. Isso o torna um fator importante no combate, podendo influenciar decisivamente para o sucesso ou fracasso de uma operação. Saber utilizá-lo de forma eficiente reveste-se de grande importância.

> Assim, a forma como o C² tem sido empregado é fator não apenas de sucesso nas operações, mas também de fracasso e derrota no combate. A tarefa de empregá-lo com eficácia revela-se, portanto, como um seguro indicador de competência na gerência do poder militar de uma nação. (BRASIL, 2015, p. 14)

Ao analisar as diversas funções que um militar da Arma de Comunicações pode desempenhar na vida administrativa de uma Organização Militar (OM), encontramos

funções importantes como a do Oficial de Informática. Essa função é descrita no Regulamento Interno e dos Serviços Gerais (RISG). Entre suas responsabilidades, pode-se observar que, para desempenhar bem sua função, o militar deve possuir um bom domínio sobre o conhecimento de Tecnologias da Informação e Comunicação (TIC). Esse fator influencia diretamente no desempenho da rede de sua OM, pois ele é o responsável pelo planejamento, manutenção, aquisição e segurança dela.

Quando se observa a formação do militar de comunicações, percebe-se que os militares temporários possuem uma carga horário muito pequena de TI. O soldado e o cabo possuem apenas 17 horas e o sargento temporário 70 horas. O 3º sargento de carreira já possui uma carga horário um pouco maior de 106 horas, porém ainda pequena se levar em consideração a importância da matéria e a quantidade de meios de comunicações que operam por meio de redes de TI. O oficial de comunicações, devido ao seu grande período de formação, possui uma carga horária total de 309 horas depois de escolhida a Arma de Comunicações, somando os 3 anos de formação. O 3º sargento, geralmente, trabalho como um operador de sistemas e, com isso, ele precisaria de uma carga horária maior para ter um conhecimento mais aprofundado sobre os sistemas com que ele trabalharia. Já o oficial, tende a trabalhar como um gestor, não necessitando de um conhecimento tão aprofundado, mas de um conhecimento mais amplo de todas as possibilidades do sistema que opera, ficando para o sargento o maior detalhamento de como fazer funcionar o sistema.

6. CONCLUSÃO

A pesquisa teve como objetivo verificar a importância do conhecimento de Redes de Tecnologia da Informação para os militares da Arma de Comunicações no século XXI. Para isso, foi realizada uma revisão bibliográfica sobre o assunto para verificar se esse conhecimento é relevante para o desempenho da função dos militares da Arma de Comunicações.

As hipóteses de pesquisa procuraram verificar se o conhecimento de redes de TI é importante para os militares da Arma de Comunicações e se possui empregabilidade para eles ou se não possui relevância para o militar da Arma de Comunicações. Dessa forma, por meio desse estudo, pode-se confirmar que o conhecimento de redes de TI é fundamental para o militar da Arma de Comunicações. Essa hipótese foi confirmada por meio das diversas situações levantadas e associadas aos possíveis empregos do conhecimento de TI. Ficou evidente que o conhecimento de TI não é apenas importante, mas fundamental para o desempenho profissional dos Comunicantes.

Com base nos dados colhidos e analisados, foi possível alcançar o objetivo geral de verificar a importância do conhecimento de Redes de Tecnologia da Informação para os militares da Arma de Comunicações no século XXI. Além disso, durante a pesquisa, foi possível observar como esse conhecimento pode influenciar o desempenho dos militares de comunicações no Exército Brasileiro, tanto na parte administrativa quanto em um cenário de guerra.

Outra situação observada, foi que, mesmo com a grande relevância do conhecimento de redes de TI, percebe-se que não há uma carga horária de instrução condizente para a consolidação desse conhecimento. Ao considerar o Oficial um gestor e o Sargento um operador do sistema de TI, o militar que mais opera diretamente os sistemas e que deveria ter um conhecimento mais aprofundado, que é o operador, possui uma carga horária de formação muito baixa. Isso pode ocasionar a formação de profissionais com deficiências na parte de redes de TI, prejudicando o desempenho profissional desse militar.

Em resumo, a pesquisa mostrou que o conhecimento de Redes de Tecnologia da Informação é fundamental para os militares da Arma de Comunicações no século XXI. Esse conhecimento pode influenciar positivamente o desempenho dos militares

de comunicações no Exército Brasileiro, tanto na parte administrativa quanto em um cenário de guerra e levantou a hipótese da possibilidade da existência de um certo déficit de carga horário na formação desses militares. Portanto, é importante que os militares da Arma de Comunicações busquem adquirir e aprimorar seus conhecimentos em Redes de Tecnologia da Informação. Esse aprimoramento é possível de ser realizado dentro da própria força por meio da Escola de Comunicações e por cursos EaD disponibilizados.

REFERÊNCIAS BIBLIOGRÁFICAS

ABDALLA, Joffre Ferreira. **A atuação do Exército Brasileiro para o domínio do espaço cibernético**. Revista do Exército Brasileiro, v. 157, n. 1, p. 2, jul. 2021.

ABDALLA, Joffre Ferreira. **Domínio do espaço cibernético por um país: uma análise da presença do Exército Brasileiro no domínio Cibernético**. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) – Escola de Aperfeiçoamento de Oficiais, Rio de Janeiro, 2020.

ACADEMIA MILITAR DAS AGULHAS NEGRAS. **Plano de disciplina (PLADIS) 2º ano/curso de comunicações.** Resende, RJ, 2021.

ACADEMIA MILITAR DAS AGULHAS NEGRAS. **Plano de disciplina (PLADIS) 3º ano/curso de comunicações.** Resende, RJ, 2021.

ACADEMIA MILITAR DAS AGULHAS NEGRAS. **Plano de disciplina (PLADIS) 4º ano/curso de comunicações.** Resende, RJ, 2021.

ARMY NATIONAL GUARD. **Control Communications.** Disponível em: <https://www.nationalguard.com/careers/technology-and-networking>. Acesso em: 16 nov. 2022.

BLUMBERG, Matthew S. **The Integrated Tactical Network: Pivoting Back to Communications Superiority**. Military Review, May-June, 2020.

BRASIL, Ministério da Defesa. **C24-16: Documentos de Comunicações**. 1. ed. Brasília, DF, 1995

BRASIL, Ministério da Defesa. **EB10-P-01.007: Plano Estratégico do Exército 2020-2023**. Brasília, DF, 2019.

BRASIL, Ministério da Defesa. **EB20-MC-10.205: Comando e Controle**. 1. ed. Brasília, DF, 2015.

BRASIL, Ministério da Defesa. **EB70-MC-10.232: Guerra Cibernética**. 1. ed. Brasília, DF, 2017.

BRASIL, Ministério da Defesa. **EB70-MC-10.241: As Comunicações na Força Terrestre**. 1. ed. Brasília, DF, 2018.

BRASIL, Ministério da Defesa. **EB70-PP-11.022: Programa-Padrão de Instrução da Formação do 3º Sargento Temporário de Comunicações**. 1. ed. Brasília, DF, 2020.

BRASIL, Ministério da Defesa. **EB70-PP-11.024: Programa-Padrão de Instrução de Qualificação do Cabo e Soldado de Comunicações**. 1. ed. Brasília, DF, 2020.

BRASIL. Portaria nº 011-DCT, de 29 de março de 2010. Aprova o Plano de Migração

para Software Livre no Exército Brasileiro, versão 2010. **Separata ao Boletim do Exército,** Brasília, DF, 30 abr. 2010.

BRASIL. Portaria nº 109, de 13 de março de 2008. Altera os Arts. 45 e 46 do Regulamento Interno e dos Serviços Gerais - R-1 (RISG), aprovado pela Portaria do Comandante do Exército nº 816, de 19 de dezembro de 2003. **Boletim do Exército**, Brasília, DF, n. 12, p. 8, 19 mar. 2008.

BRASIL, Exército Brasileiro. Portaria Nº 193-EME, de 22 de dezembro de 2010. Aprova a Diretriz para a Implantação do Projeto Sistema Integrado de Monitoramento de Fronteiras (SISFRON). **Boletim do Exército**. Disponível em: <http://www.sgex.eb.mil.br/sistemas/boletim_do_exercito/boletim_be.php>. Acesso em: 4 jul. 2023.

BRASIL. Portaria nº 3,781/GM-MD, de 17 de novembro de 2020. Cria o Sistema Militar de Defesa Cibernética (SMDC) e dá outras providências. **Diário Oficial da União**, Brasília, DF, n. 221, 19 nov. 2020. Seção 1, p. 12.

BURKEN, Christine G. van. **A Tecnologia Não é Neutra: O Perigo Imprevisto das Operações Capacitadas por Redes.** Military Review Edição Brasileira Julho-Agosto, 2013.

CHAVES, Matehus Nery. A formação dos recursos humanos para operação dos meios de tecnologia da informação no Exército Brasileiro: proposta de atualização das instruções de redes de computadores para os cabos e soldados de comunicações. **O Comunicante**, Brasília, v. 12, n. 1, 2022.

COMPUGRAF. **Guerra Cibernética e os conflitos na era da Informação,** 2020. Disponível em: <https://www.compugraf.com.br/guerra-cibernetica/>. Acesso em: 11 jul. 2023.

DE LIMA, Denis Lucio. **Implantação da ferramenta Zabbix no Centro de Avaliações do Exército – CAEx, como plataforma de gestão e monitoramento do ambiente computacional, na prevenção a sinistros na rede**. Trabalho de Conclusão de Curso (Especialização em Ciências Militares) – Escola de Formação Complementar do Exército, Rio de Janeiro, 2020.

DA SILVA, Gilmar Pereira. **Guerra Cibernética: preparo e emprego do exército**. Trabalho de Conclusão de Curso (Especialização em Política, Estratégia e Administração Militares) – Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2006.

DA SILVA, Júlio Cezar Barreto Leite. **Guerra Cibernética: A guerra no Quinto Domínio, conceituação e princípios**. Revista Escola de Guerra Naval, Rio de Janeiro, v. 20, n. 1, p. 193-211, jan./jun. 2014.

ESCOLA DE COMUNICAÇÕES. **Missão**. Brasília, 2022. Disponível em: <http://www.escom.eb.mil.br/missao>. Acesso em: 5 jul. 2023.

ESCOLA DE SARGENTOS DAS ARMAS. **Currículo do Curso de Formação e Graduação de Sargentos (CFGS) - 2º Ano: Comunicações.** Três Corações, MG, 2021.

EXÉRCITO, Centro de Comunicação Social do Exército. **Dia da Arma de Comunicações – 5 de maio**, Brasília, DF, 2022. Disponível em: < https://www.eb.mil.br/documents/10138/14839249/DIA+DAS+COM+2022.pdf/a49cd92b-4ea5-5026-6dd0-7b2dbf5d20e3>. Acesso em: 13 nov. 2022.

FINNEY, Nathan K. **"The Modern Military Profession," in Redefining the Modern Military: The Intersection of Profession and Ethics.** MD: Naval Institute Press, Annapolis, 2018.

GROSSO, C. R. N.; GOMES, C. A. S.; SILVA, S. W.. As novas tecnologias da informação e comunicação e seus impactos gerenciais no âmbito do Exército Brasileiro. **Revista Brasileira de Administração Científica**, v.10, n.1, p.57-68, 2019. Disponível em: <http://doi.org/10.6008/CBPC2179-684X.2019.001.0005>. Acesso em: 5 jul. 2023.

HARRIS, **Treinamento Sistema MTO**. [s.l.: s.n.], 2013.

HIRSCHKORN, Jared. **Project divergence:** reimagining army capabilities in the era of network technology. Modern War Institute at West Point, New York, 2022. Disponível em: <https://mwi.usma.edu/project-divergence-reimagining-army-capabilities-in-the-era-of-network-technology/>. Acesso em: 16 nov. 2022.

IGREJA, Arthur. **Como a tecnologia afeta diferentes dimensões da guerra**, 2022. Disponível em: <https://epocanegocios.globo.com/colunas/noticia/2022/03/como-tecnologia-afeta-diferentes-dimensoes-da-guerra.html>. Acesso em: 16 jun. 2023.

JÚNIOR, Célio Pires de Oliveira. **Monitoração de sistemas:** uso de ferramentas gratuitas para gerenciar uma rede de computadores. Trabalho acadêmico (Especialização em Ciências Militares) – Escola de Aperfeiçoamento de Oficiais, Rio de Janeiro, 2018.

JÚNIOR, Armando Kolbe. **Brasil teve mais de 1,6 bilhão de ataques cibernéticos em três meses**, 2020. Disponível em: <https://www.uninter.com/noticias/brasil-teve-mais-de-16-bilhao-de-ataques-ciberneticos-em-tres-meses>. Acesso em: 5 jul. 2023.

MENDES, Tatyane. **TI: Entenda de uma vez o que é a Tecnologia da Informação**, 2022. Disponível em: <https://www.napratica.org.br/ti-entenda-de-uma-vez-o-que-e-a-tecnologia-da-informacao>. Acesso em: 6 mar. 2023.

MORTON, Michael S. Scott. **The corporation of the 1990s: information technology and organizational transformation**. New York, Oxford University Press, 1991.

NETACAD, **Cursos**. Disponível em: <https://www.netacad.com/pt-br/courses/all-courses>. Acesso em: 10 jul. 2023.

NOTO. **Virtualização com PROXMOX:** Tudo sobre ela, 2022. Disponível em: <https://nototidigital.com.br/2022/08/10/virtualizacao-com-proxmox-tudo-sobre-ela/>. Acesso em: 7 jul. 2023.

PACETE, Luiz Gustavo. **5 ataques cibernéticos no Brasil em 2021 que geraram alerta**, 2021. Disponível em: <https://forbes.com.br/forbes-tech/2021/12/5-ataques-ciberneticos-no-brasil-em-2021-que-geraram-alerta/>. Acesso em: 14 jul 2023.

PINHEIRO, Alvaro de Souza. **A Tecnologia da Informação e a Ameaça Cibernética na Guerra Irregular do Século XXI**. Artigo Científico, Rio de Janeiro, 2008.

PPLWARE. **OpenMeetings – A melhor plataforma open source para reuniões online?**, 2018. Disponível em: <https://pplware.sapo.pt/internet/aprenda-a-instalar-o-openmeetings-um-sistema-web-para-conferencias/#:~:text=O%20OpenMeetings%20é%20uma%20plataforma%20open%20source%2C%20escrita,certamente%20a%20melhor%20produtividade%20das%20equipas%20de%20trabalho.>. Acesso em: 10 jul. 2023.

PT.LINUX. **Remmina - Uma ferramenta de compartilhamento de área de trabalho remota rica em recursos para Linux.** Disponível em: <https://pt.linux-console.net/?p=1836#gsc.tab=0>. Acesso em: 10 jul. 2023.

SAN, Blog. **O que é Zimbra E-mail? Conheça as vantagens e todos os recursos,** 2022. Disponível em: <https://blog.saninternet.com/o-que-e-zimbra>. Acesso em: 14 jul. 2023.

SOUZA, L. B. **Gerenciamento e segurança de redes**: Tecnologia da Informação. São Paulo: SENAI, 2017.

SUZUKI, Shin. **A guerra cibernética paralela entre Rússia e Ucrânia**, 2022. Disponível em: <https://www.bbc.com/portuguese/internacional-60551648>. Acesso em: 14 jul. 2023.

TELECOM, Algar. **Tecnologia da Informação e Comunicação (TIC):** O que são?, 2022. Disponível em: <https://blog.algartelecom.com.br/inovacao/significado-de-tics-entenda-de-uma-vez-por-todas/>. Acesso em: 5 jul. 2023.

TIDY, Joe. **Guerra na Ucrânia: os três ciberataques russos que as potências ocidentais mais temem.** Disponível em: <https://www.bbc.com/portuguese/internacional-60843427>. Acesso em: 14 jul. 2023.

TRINDADE, Rodrigo. **Guerra 2.0, o futuro chegou**, 2019. <https://www.uol.com.br/tilt/reportagens-especiais/novas-tecnologias-irao-moldar-guerra-do-amanha/#cover>. Acesso em: 16 jun. 2023.

VALLE, B. de M. Tecnologia da informação no contexto organizacional. **Ciência da**

Informação, *[S. l.]*, v. 25, n. 1, 1996. Disponível em: <https://revista.ibict.br/ciinf/article/view/669>. Acesso em: 9 nov. 2022.