ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO
ESCOLA MARECHAL CASTELLO BRANCO

Maj Com VICTOR DE **MATOS** VASCONCELOS CARVALHO

UMA PROPOSTA DE PROTEÇÃO CIBERNÉTICA PARA O MÓDULO DE TELEMÁTICA OPERACIONAL

Rio de Janeiro
2022

Maj Com VICTOR DE **MATOS** VASCONCELOS CARVALHO

UMA PROPOSTA DE PROTEÇÃO CIBERNÉTICA PARA O MÓDULO DE TELEMÁTICA OPERACIONAL

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Defesa.

Orientador: Maj Art QEMA Felipe Galvão Franco Honorato

Rio de Janeiro
2022

C331p Carvalho, Victor de Matos Vasconcelos.

Uma proposta de proteção cibernética para o módulo de telemática operacional. / Victor de Matos Vasconcelos Carvalho.–2022.

42 f. : il. ; 30 cm.

Orientação: Felipe Galvão Franco Honorato.

Trabalho de Conclusão de Curso (Especialização em Ciências Militares) –Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2022.

Bibliografia: f. 39-40

1. Proteção Cibernética. 2. Módulo de telemática operacional. 3. Segurança. I. Título.

Maj Com VICTOR DE **MATOS** VASCONCELOS CARVALHO

UMA PROPOSTA DE PROTEÇÃO CIBERNÉTICA PARA O MÓDULO DE TELEMÁTICA OPERACIONAL

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Defesa.

Aprovado em ___ de novembro de 2022.

COMISSÃO AVALIADORA

_____
Felipe Galvão Franco Honorato – Maj Art QEMA- Presidente
Escola de Comando e Estado-Maior do Exército

_____
Fábio de Souza e Silva– Ten Cel Inf QEMA - Membro
Escola de Comando e Estado-Maior do Exército

_____
Daniel Ramos Lemos – Maj QEMA - Membro
Escola de Comando e Estado-Maior do Exército

A minha família, esteio de segurança e felicidade, que me forneceram a energia e o equilíbrio necessário para vencer os desafios dessa difícil jornada.

.

AGRADECIMENTOS

A Deus, pela saúde e força espiritual que me acompanha durante esse curso que tanto quis realizá-lo.

À minha esposa Maria Angélica por ter me apoiado nessa decisão e aos meus filhos Gustavo e Gabriela por terem deixado estudar durante as noites e no final de semana. Aos três, as minhas desculpas pela ausência nesse período.

Aos meus pais Sebastião e Marilena pela torcida e pela vibração de mais uma conquista do seu filho.

Por fim, agradeço ao Major Felipe Galvão Franco Honorato pelas orientações seguras durante a realização desse trabalho.

“O sucesso é a soma de pequenos esforços
repetidos dia após dia.”
Robert Collier.

RESUMO

O Exército Brasileiro por meio do Projeto SISFRON (Sistema Integrado de Monitoramento de Fronteiras), cujo principal objetivo é monitorar e vigiar as fronteiras do país em tempo real, além de propiciar uma resposta rápida para qualquer risco, adquiriu múltiplos equipamentos como radares, sensores, viaturas e um sistema de comando e controle para aumentar a consciência situacional aos comandantes. A aquisição do Módulo de Telemática Operacional foi uma peça fundamental para esse objetivo. Tal capacidade permite a comunicação de dados, voz e imagens, criando redes de computadores nas Operações Militares. Além disso, possibilita as comunicações via rádio, integração à rede pública de telefonia fixa ou celular, transmissão de vídeo a dezenas de quilômetros, acesso à Internet com até 100 km de distância da base de operações, emprego de tecnologia VoIP (Voz sobre IP) e integração a qualquer cenário remoto através de sistemas de comunicações via satélite. Com toda essa capacidade de comunicações em redes, além da aquisição do Módulo de Telemática Operacional, houve a necessidade de capacitar os militares para operarem esse recurso de alto nível tecnológico. para isso publicou em 2015, o Caderno do Instrução EB70-CI-11.406 – Caderno de Instrução do Operador do Módulo de Telemática Operacional, onde aborda as configurações básicas dos equipamentos, porém não aborda assuntos de proteção cibernética como os de segurança no switch e do roteador. Nesse interim, foi realizado um trabalho em 2018, no Centro de Instrução de Guerra Eletrônica, onde esses equipamentos foram explorados e atacados ciberneticamente, na qual foram encontradas vulnerabilidades. No intuito de aprimorar a proteção cibernética do Módulo de Telemática Operacional, esse trabalho pretende realizar a mitigação dessas vulnerabilidades encontradas, propondo sua proteção cibernética.

Palavras-chave: 1. Proteção Cibernética. 2. Módulo de Telemática Operacional. 3. Segurança.

.

ABSTRACT

Brazilian Army, through the SISFRON Project (Integrated Border Monitoring System), where its main objective is to monitor and guard the country's borders in real time, as well as providing a quick response to any risk. In order to fulfill this task, Brazilian Army acquired multiple pieces of equipment, such as radars, sensors, vehicles and a command-and-control system, to increase the situational awareness of commanders. The acquisition of the Operational Telematics Module was a key part of this objective. Such capability allows the transmission of data, voice and images, creating computer networks in Military Operations. Besides, it enables radio communications, integration into the public fixed or cellular telephone network, video transmission over dozens of kilometers, Internet access up to 100 km away from the base of operations, usage of VoIP (Voice over IP) technology. and integration to any remote scenario through satellite communications systems. With all this communication capacity in networks, in addition to the acquisition of the Operational Telematics Module, there was a need to train the soldiers to operate this high technological level resource. For this, in 2015, it was published the Instruction Manual EB70-CI-11.406 – Operational Telematics Module Operator's Instruction Manual, where it addresses the basic configurations of the equipment, but does not address cybernetic protection issues, such as security on the switch and router. In the meantime, a cyber action was carried out, in 2018, at the Electronic Warfare Instruction Center, where this equipment was exploited and attacked cybernetically, exposing some vulnerabilities. In order to improve the cybernetic protection of the Operational Telematics Module, this work aims to mitigate these vulnerabilities found, proposing cybernetic protection and other solutions.

Keywords: 1. Cyber Protection. 2. Operational Telematics Module. 3. Security.

LISTA DE ABREVIATURAS

ARP	*Adress Resolution Protocol*
ARP Spoofing	*Adress Resolution Protocol Spoofing*
C2	Comando e Controle
CComGEx	Comando de Comunicações e Guerra Eletrônica
CDP	*Cisco Discovery Protocol*
DHCP	*Dynamic Host Configuration Protocol*
DoS	*Denial of Service*
EB	Exército Brasileiro
EBNet	Rede Privada do Exército Brasileiro
END	Estratégia Nacional de Defesa
ERB	Estação Rádio Base
FA	Forças Armadas
FAMES	Flexibilidade, Adaptabilidade, Modularidade, Extensibilidade e Sustentabilidade
F Ter	Força Terrestre
G Ciber	Guerra Cibernética
GCR	Guerra Centrada em Redes
HF	*Hight Frequency*
LBDN	Livro Branco de Defesa Nacional
MAC	*Media Access Control*
MD	Ministério da Defesa
MEM	Material de Emprego Militar
MPC	Módulo de Proteção Cibernética
MTO	Módulo de Telemática Operacional
NA	Nó de Acesso
OSI	*Open System Interconection*
SAM	Sistema de Assinante Móvel
SCA	Sistema de Comunicações de Área
SCC	Sistema de Comunicações de Comando
SC²FTer	Sistema de Comando e Controle da Força Terrestre
SISFRON	Sistema de Fronteiras
SISTAC	Sistema de Comunicações Táticas
SSH	*Secure Socket Shell*
STP	*Spanning Tree Protocol*
ROD	Rede Operacional de Defesa
PC	Posto de Comando
VLAN	*Virtual Local Area Network*
VHF	*Very Hight Frequency*
VoIP	Voz sobre IP
Z Aç	Zona de Ação

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

A proteção cibernética do Módulo de Telemática Operacional (MTO) é uma necessidade no contexto da Guerra Centrada em Redes (GCR). Tal ação justifica-se a atual conjuntura internacional, onde os ataques cibernéticos têm crescido a cada ano. O Brasil foi o 5º País que mais sofreu ataques cibernéticos no ano de 2021, gerando perdas incalculáveis para empresas e ao governo brasileiro. (PRADO, F., 2022)

O Exército Brasileiro, cumprindo as orientações da Estratégia Nacional de Defesa de 2016 (END), documento no qual orienta as questões de defesa e as ações necessárias para efetivamente dotar o Estado da capacidade para atender seus interesses, busca aumentar a sua capacidade de proteção, na qual garante a soberania, o patrimônio nacional e a integridade territorial no espaço cibernético.

Os programas estratégicos conhecidos como o Sistema Integrado de Monitoramento de Fronteiras (SISFRON) e o Defesa Cibernética permitem o processo de transformação do Exército Brasileiro. Essa obtenção de novas capacidades, sob a orientação das características doutrinárias regidas pelo acrônimo FAMES: flexibilidade, adaptabilidade, modularidade, elasticidade e sustentabilidade aumentaram a escalabilidade e a capilaridade do Sistema de Comando e Controle da Força Terrestre (SC2FTer).

Incumbiu ao SISFRON de monitorar e vigiar as fronteiras do País em tempo real, além de garantir resposta rápida para qualquer risco. Para cumprir essa incumbência, o Exército Brasileiro adquiriu diversos equipamentos como radares, sensores, viaturas e um sistema de comando e controle para proporcionar a consciência situacional aos comandantes. Uma peça fundamental para as comunicações foi a obtenção do Módulo de Telemática Operacional.

O MTO permite a comunicação de dados, voz e imagens, criando redes de computadores nas Operações Militares. O MTO possibilita ainda às comunicações via rádio, integração à rede pública de telefonia fixa ou celular, transmissão de vídeo a dezenas de quilômetros, acesso à Internet a centenas de quilômetros de distância da base de operações, emprego de tecnologia VoIP (Voz sobre IP) e integração a qualquer cenário remoto através de sistemas de comunicações via satélite. (HARRIS, 2014)

Cabe a Defesa Cibernética as atividades ofensivas, defensivas e exploratórias realizadas no espaço cibernético, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional. (BRASIL, 2014)

Nesse sentido, o problema das informações transitadas no MTO não estarem protegidas poderá expor ativos de informação tais como: dados que transitam nos sistemas de Comando e Controle, dados pessoais e coorporativos que estão nos computadores e servidores do Exército Brasileiro. Dessa forma, informações que poderiam auxiliar a tomada de decisão dos comandantes poderão ser utilizadas por outros atores, reduzindo a vantagem no campo de batalha.

Nesse contexto, o Exército Brasileiro necessitou capacitar os militares para operarem esse recurso de alto nível tecnológico. Para isso foi publicado em 2015 o Caderno do Instrução EB70-CI-11.406 – Caderno de Instrução do Operador do Módulo de Telemática Operacional, onde aborda as configurações básicas dos equipamentos contidos no MTO, porém foi verificado que a proteção cibernética não foi evidenciada. Além disso, a alta complexidade de configuração, a necessidade de entender o idioma inglês para atualizar-se frente as novidades cibernéticas e a alta rotatividade dos militares nas Organizações Militares (OM) do Exército Brasileiro tem dificultado a manutenção da Proteção Cibernética nesses equipamentos.

Nesse interim, foi realizado uma pesquisa por Carvalho (2018) buscando verificar os impactos de comando e controle no switch do MTO por meio de ataques cibernéticos em redes operacionais sendo concluído que o MTO está vulnerável e necessita de mecanismos de proteção cibernética.

Dessa forma, no intuito de proteger os dados trafegados no SC2FTer e negar os ataques e as explorações cibernéticas nos dispositivos do MTO, esse trabalho visa a solucionar essas vulnerabilidades existentes com uma proposta de proteção cibernética, contribuindo para a segurança dos dados trafegados por esses dispositivos.

1.1 PROBLEMA

A Força Terrestre (F Ter) utiliza o MTO como meio de receber e transmitir os dados das Operações Militares. Esses dados propiciam a consciência situacional do comandante como informações do campo de batalha.

Segundo Carvalho (2018), após realizar ataques cibernéticos no MTO foi concluído que existem diversas vulnerabilidades que podem impactar o funcionamento do módulo, causando prejuízos no SC2FTer.

Desse modo, fica evidente que é imprescindível a realização de um trabalho para que seja mitigado essas vulnerabilidades, contribuindo para a manutenção da segurança, princípio fundamental para o C2.

Com base no exposto acima, cabe formular o seguinte problema:

Como mitigar as vulnerabilidades cibernéticas encontradas no Módulo de Telemática Operacional?

1.2 OBJETIVOS

Objetivo geral - O presente estudo pretende propor medidas de proteção cibernéticas para o MTO.

Objetivos específicos -

a. Estudar os assuntos relacionados a Proteção do MTO;

b. Descrever as vulnerabilidades encontradas no MTO e relacioná-las aos seus impactos de C2;

c. Propor medidas para mitigar essas vulnerabilidades conhecidas.

1.3 DELIMITAÇÃO DO ESTUDO

O presente estudo propõe formas para mitigar as vulnerabilidades encontradas por Carvalho (2018) em seu trabalho, onde foi realizado ataques cibernéticos em redes operacionais de C2 no switch do MTO. Assim, o foco desse trabalho será no aumento da segurança desses equipamentos de comunicações.

1.4 RELEVÂNCIA DO ESTUDO

O Exército Brasileiro cumprindo as orientações do Livro Branco de Defesa Nacional (LBDN) (2012), documento no qual orienta as questões de Defesa e as ações necessárias para efetivamente dotar o Estado da capacidade para atender seus interesses, busca aumentar a sua capacidade de proteção, na qual garante a soberania, o patrimônio nacional e a integridade territorial no espaço cibernético.

> O espaço cibernético tem sido amplamente empregado nos conflitos da atualidade como um dos meios pelos quais os Estados em beligerância buscam obter vantagens sobre seu oponente. Em um mundo cada vez mais dependente da tecnologia em rede, as preocupações com a segurança da informação no Exército Brasileiro tornam-se crescentes, especialmente no tocante às informações que transitarão nos sistemas de comando e controle da Força Terrestre, em caso de um conflito envolvendo o Brasil. (DOS SANTOS, 2021)

Dessa forma, o Exército Brasileiro possui o desafio de ampliar o grau de segurança das informações transitadas nos sistemas de comando e controle a fim de estar preparado para enfrentar as ameaças cibernéticas que ocorrem hoje e no futuro, em um ambiente cada vez mais dependentes da tecnologia da informação e comunicações, como pode ser observado pelo estudo prospectivo dos cenários de defesa para os anos de 2020 a 2039, realizado pelo Ministério da Defesa:

> Com as operações militares centradas em redes e, como tal, dependentes de sistemas de comunicação e informação, haverá incremento da guerra cibernética. A necessidade de garantir o uso do domínio informacional e impedir que o oponente o faça (Superioridade da Informação) se incrementará. Ataques cibernéticos serão também utilizados contra infraestruturas nacionais – governamentais, econômicas e militares – que suportam o esforço de guerra. (BRASIL, 2017, p.21)

2. METODOLOGIA

Nessa seção, será apresentada a metodologia utilizada para desenvolver o trabalho, evidenciando-se os seguintes tópicos: tipo de pesquisa, universo e amostra, coleta de dados, tratamento de dados e limitações do método.

2.1 TIPO DE PESQUISA

Trata-se de uma pesquisa exploratória tendo em vista que se visa, inicialmente, uma maior aproximação com o tema e de uma pesquisa explicativa. As melhores práticas empregadas no mercado global de defesa foram empregadas como mecanismos para mitigar os efeitos dos ataques cibernéticos no Módulo de Telemática Operacional em uma rede de C2. Quanto ao seu método, classificar-se-á em hipotético-dedutivo pois será estabelecido hipóteses para resolver os problemas apresentados e depois serão revisados por meio da literatura. Quanto à abordagem como qualitativa, quanto à finalidade como aplicada e quanto aos procedimentos como uma pesquisa bibliográfica e um estudo de caso.

É feita uma revisão bibliográfica acerca do funcionamento do Módulo de Telemática Operacional, das tarefas de ataques e proteção cibernética, das vulnerabilidades encontradas no roteador no MTO e de uma proposta de proteção cibernética a fim de mitigar essas vulnerabilidades.

2.2 UNIVERSO E AMOSTRA

O universo do presente estudo serão os equipamentos físicos de rede que compõe o MTO distribuídos pelo Comando de Comunicações e Guerra Eletrônica do Exército (CComGEx) às OM de Comunicações.

A amostra escolhida serão os equipamentos do MTO configurados com todas as especificações do Caderno do Instrução EB70-CI-11.406, o que garantirá a obediência aos requisitos técnicos propostos de utilização, garantindo as mesmas condições de utilização pelas OM operativas.

2.3 COLETA DE DADOS

A reunião dos dados do presente trabalho de conclusão de curso dar-se-á por meio de coleta na literatura, realizando-se uma pesquisa bibliográfica nos manuais do EB e de pesquisas correlatas com o assunto. Os dados colhidos na bibliografia fundamentarão a explicação sobre o funcionamento do Comando e Controle, da Proteção Cibernética no Exército e do funcionamento do MTO. Além disso, com base nesse trabalho de conclusão de curso de Carvalho objetiva-se criar mecanismos de proteção aos ataques cibernéticos nos dispositivos do MTO buscando formas de inibir os impactos de comando e controle.

2.4 TRATAMENTO DOS DADOS

O método de tratamento de dados que será utilizado no presente estudo será o estudo dos ataques cibernéticos bem como os impactos na rede de C2, após o relacionamento de causa e efeito será buscado a solução para mitigar essa consequência, por meio da leitura bibliográfica dos manuais do roteador da família 2900 da CISCO e de trabalhos que abordam sobre a proteção cibernética desse equipamento.

2.5 LIMITAÇÕES DO MÉTODO

A metodologia em questão possui limitações, particularmente, quanto à pesquisa bibliográfica uma vez que o tema é de estrito interesse das Forças Armadas, sendo difícil o acesso as bibliografias atinentes ao MTO. Todavia, a proteção cibernética dos dispositivos de redes tem vasta bibliografia na rede mundial de computadores. Dessa forma, nesse trabalho será feito uma ligação dos métodos civis de segurança de redes com os atuais equipamentos militares contidos no MTO.

3. REFERENCIAL BIBLIOGRÁFICO

Neste capítulo, serão abordados os principais conceitos relacionados a redes de computadores, Guerra Cibernética, Sistemas de C2 baseados em redes, Guerra Centrada em Redes, MTO e o MTO no Sistema de Comunicações Táticas.

3.1 REDES DE COMPUTADORES

Uma rede de computadores é um conjunto de computadores interligados entre si por um sistema de comunicação, ou seja, é um conjunto de enlaces físicos e lógicos entre vários *hosts* ou dispositivos. Os objetivos básicos de uma rede de computadores são: trocar dados e compartilhar dispositivos. (TANENBAUM, 2003).

De uma forma didática, rede de computadores pode ser visualizada como uma rede de estradas que conectam grupos de pessoas criando uma rede física, e que as redes de computadores consistem em uma série de dispositivos, sendo que alguns podem servir como *hosts*. Um *host* é qualquer dispositivo que envia e recebe informações na rede. (ODOM, 2016).

Para que as redes de computadores funcionem, é necessário que exista uma comunicação clara entre os dispositivos, ou seja, com protocolos padronizados. Dessa forma, foi criado o modelo de *Open System Interconnection (OSI)*, ou também conhecido como, Interconexão de Sistemas Abertos a fim de padronizar a comunicação.

A seguir, será explicado como é o funcionamento desse modelo conceitual, para que mais a frente possamos entender em qual nível as ameaças afetam o MTO e quais ferramentas atinentes as camadas de rede podemos utilizar para proteger os dados.

3.2 O MODELO DE INTERCONEXÃO DE SISTEMAS ABERTOS (OSI)

No início dos anos 1980, a Organização Internacional para Padronização (ISO) desenvolveu o modelo de referência *OSI* (*Open Systems Interconnect* - Interconexão de Sistemas Abertos) para padronizar a forma como os dispositivos se comunicam em uma rede. Esse modelo foi um passo importante para garantir a interoperabilidade entre dispositivos de rede.

Segundo Odom:

> [...] *ISO*, a Organização Internacional de Padronização, é o maior desenvolvedor de padrões internacionais do mundo para uma grande variedade de produtos e serviços. *ISO* não é uma sigla para o nome da organização. O termo *ISO* baseia-se na palavra grega “isos”, que significa igual. A Organização Internacional para Padronização escolheu o termo ISO para afirmar sua posição como sendo igual em todos os países.(ODOM, 2016, p 23).

Diógenes e Mauser dizem que:

> [...] em redes, *ISO* é mais conhecido por seu modelo de referência da Interconexão de Sistemas Abertos (*OSI*, *Open Systems Interconnection*). A ISO publicou o modelo de referência OSI em 1984 para desenvolver uma estrutura em camadas para protocolos de rede. O objetivo original deste projeto era não só criar um modelo de referência, mas também funcionar como uma base para um conjunto de protocolos a serem usados para a Internet. Isso ficou conhecido como o conjunto de protocolos do OSI.(DIÓGENES; MAUSER, 2015, p. 27).

Modelo OSI

Modelo OSI	Camada	Descrição
Aplicação	7	Responsável por fornecer serviços de rede às aplicações
Apresentação	6	Transforma formatos de dados a fim de disponibilizar uma interface padrão para a camada de aplicação
Sessão	5	Estabelece, gerencia e encerra as conexões entre a aplicação local e a remota
Transporte	4	Oferece transporte confiável e controle de fluxo em uma rede
Rede	3	Responsável por endereçamento lógico e roteamento de domínios
Enlace de Dados	2	Oferece procedimentos de endereçamento físico e acesso ao meio
Física	1	Define todas as especificações físicas e elétricas dos dispositivos

Figura 1 - Descrição das sete camadas do Modelo de Referência OSI. *Fonte: Filippeti (2014).*

O modelo *OSI* divide as comunicações de rede em sete camadas distintas, como mostrado na Figura 1. Embora existam outros modelos, a maioria dos fornecedores de rede hoje em dia cria seus produtos usando essa estrutura.

Filippetti diz ainda que:

> [...]o modelo OSI, basicamente, divide as tarefas inerentes à transmissão de informações entre máquinas em rede em sete grupos ou “camadas”. A vantagem imediata dessa divisão é a geração de grupos menores e, portanto, mais facilmente gerenciáveis, em detrimento de apenas um pesado e complexo grupo. Como já dizia Sun Tzu no livro “A Arte da Guerra”: Dividir para conquistar.
> Cada camada é razoavelmente independente das demais, permitindo, por exemplo, que tarefas associadas a uma camada possam ser implementadas ou modificadas sem que as demais tenham que sofrer qualquer tipo de alteração. (FILIPPETTI, 2014, p. 39).

A seguir, será explicado brevemente a função de cada camada do modelo OSI, iniciando pela camada sete do modelo OSI, pelo motivo que, geralmente, é nessa camada que começa a interação usuário-máquina e facilitará o entendimento.

3.2.1 Camada de Aplicação – camada sete

É nessa camada que ocorre a interação “usuário-máquina”. A camada de aplicação é responsável por identificar e estabelecer a disponibilidade da aplicação na máquina destinatária e alocar os recursos para que tal comunicação aconteça. Exemplos de aplicações: navegadores web (Google Chrome, Mozzila Firefox, Safari, Microsoft Edge) que permitem que o usuário naveguem nas aplicações de C2, por exemplo.

3.2.2 Camada de Apresentação – camada seis

A camada de apresentação responde as solicitações da Camada de Aplicação e encaminha o serviço para a camada imediatamente inferior (sessão).

A camada de apresentação tem a função de formatar, interpretar os dados, bem como a compressão, descompressão, encriptação e decriptação dos dados.

3.2.3 Camada de Sessão – camada cinco

A camada de sessão é responsável pelo estabelecimento, gerenciamento e finalização de sessões entre a entidade transmissora e a entidade receptora.

3.2.4 Camada de Transporte – camada quatro

Os serviços definidos na camada de transporte são responsáveis pela segmentação e reconstrução dos fluxos de dados provenientes das camadas superiores. Eles provêm comunicação ponto a ponto entre aplicações, podendo estabelecer uma comunicação lógica entre a aplicação origem e aplicação destino em uma rede.

A camada de Transporte também é responsável pela disponibilização de mecanismos para multiplexar, ou seja, transmitir diversas informações

simultaneamente usando-se o mesmo canal, os fluxos de dados de camadas superiores. (FILIPPETTI, 2014, p. 65).

Nessa camada, dois protocolos de comunicação são os mais utilizados: o protocolo UDP (sigla para *User Datagram Protocol*) tem, como característica essencial, a falta de confiabilidade, porém sua velocidade é muito importante para a comunicação, a videoconferência e o uso do telefone voip são exemplos da utilização do protocolo UDP. O protocolo TCP é, talvez, o mais utilizado na camada de transporte para aplicações na Web. Diferente do UDP, o TCP é voltado à conexão e tem como garantia a integridade e ordem de todos os dados. A navegação em sites da Internet, envio de e-mail, ou conversas em servidores de chat, são exemplos da utilização do protocolo TCP.

3.2.5 Camada de Rede – camada três

A camada de Rede é responsável pelo roteamento dos dados através da rede e pelo endereçamento lógico dos pacotes de dados, ou seja, pelo transporte de tráfego entre máquinas que se encontram em redes distintas. Roteadores, também chamados de dispositivos de camada 3, são definidos nessa camada e provêm todos os serviços relacionados ao processo de roteamento. (TANENBAUM, 2003).

O processo de roteamento é interligar redes de computadores distintas, e o principal dispositivo utilizado é o roteador que tem a capacidade de ler endereços lógicos, conhecidos também como endereço IP (*Internet Protocol*) para direcionar esse pacote para o caminho do destino.

3.2.6 Camada de Enlace de Dados – camada dois

A camada de enlace tem papel importante pois,

> [...] faz a “ponte” entre a camada superior (Rede) e a camada inferior (Física), tornando possível a transmissão através de meios físicos diversos. A camada de Enlace formata a mensagem em frames e adiciona um cabeçalho próprio contendo, entre outras informações, o endereço de hardware, ou endereço físico também conhecido como *MAC address* da máquina transmissora e da destinatária. (FILIPPETTI, 2014, p. 49).

Assim como roteadores, são definidos na camada de Rede, na camada de enlace temos os *switches*, que são elementos de rede que interpretam apenas informações da camada de enlace, ignorando por completo os cabeçalhos das

camadas superiores. Aos *switches* não importa o endereço IP do destino, mas o endereço físico do mesmo.

3.2.7 Camada Física – camada um

A camada física é definida como os meios físicos de acesso, como os cabos de par trançado, fibra ótica e rádio. (ODOM, 2016).

O equipamento definido na camada Física é a placa de rede de um computador ou o *hub,* elemento muito comum em um passado não muito distante. Os *hubs* são nada mais que repetidores elétricos com múltiplas portas. Sua função se resume em receber um sinal, amplificá-lo e repassá-lo para todas as suas portas ativas, sem qualquer exame dos dados no processo. Isso significa que todos os dispositivos conectados a um *hub* conseguem receber todas os dados enviados pelos outros dispositivos.

3.2.8 Roteador CISCO 2921 no modelo *OSI*

O Roteador CISCO 2921 como qualquer outro roteador trabalha até a camada de rede, ou camada três do modelo OSI. Isso quer dizer que quando um pacote é recebido em uma determinada interface do roteador, o endereço de destino é conferido. Se o pacote destinado a uma rede não estiver na tabela de roteamento ele irá descartar, caso o pacote destinado a uma rede estiver em sua tabela de roteamento ele irá encaminhar para a interface de destino. (FILIPPETTI, 2014).

O objetivo do roteador é interligar redes diferentes, no caso do roteador CISCO 2921 do MTO é interligar Batalhões e Brigadas (HARRIS, 2014), dessa forma o roteador 2921 tem papel fundamental de conectar as Unidades e Grandes Unidades nas redes de C2.

Na figura 2, fica evidente a função do roteador no MTO, ele faz a ligação de Unidades diferentes, por meio de conexões diferentes, como no exemplo temos telefones VoIP, rádios, *laptops* e dados.

Cada Unidade é uma rede diferente, esse sistema permite a rapidez da transmissão da informação, contribuindo para a consciência situacional dos comandantes.

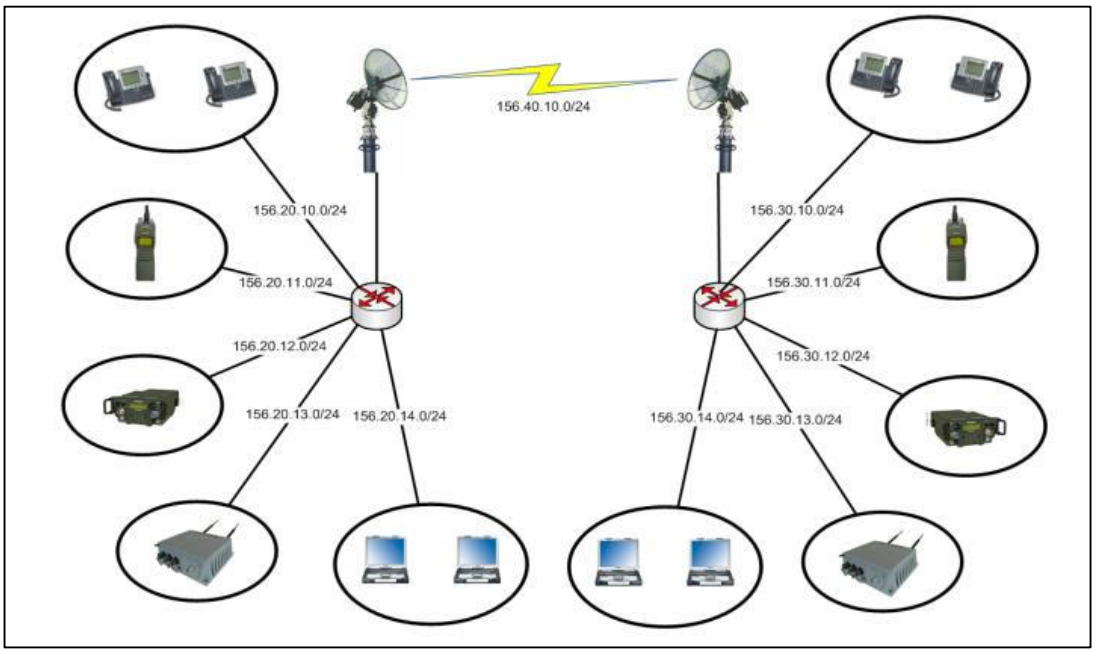

Figura 2 - Funcionamento do roteador e do switch no MTO. Fonte: Harris, (2014).

Quando se diz que o roteador trabalha até a camada de rede, quer dizer que além de entender os protocolos desta camada, ele entende as camadas mais baixas, que são a camada de enlace e a camada física. As camadas superiores (acima da camada de rede no modelo *OSI*) não são interpretadas pelo roteador em sua funcionalidade principal, porém pode-se ativar alguns protocolos de camada superior, tais como: protocolo TCP e UDP da camada de transporte, e protocolo TELNET, SSH e SNMP da camada de aplicação.

O roteador 2921 possui também um módulo de switch de vinte e quatro portas acoplado com o objetivo de conectar dispositivos locais como computadores, telefones e equipamentos de vídeo conferência. (HARRIS, 2014)

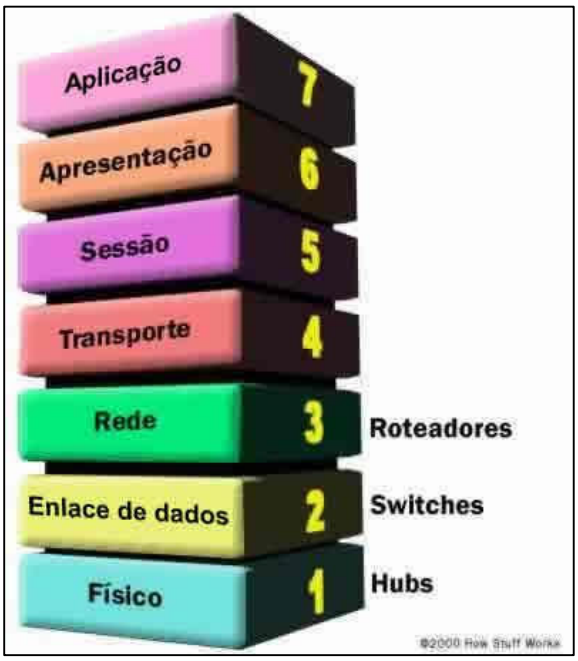

Figura 3 - Representação do roteador e do switch no modelo OSI. Fonte: Prado W. (2009).

3.3 SISTEMAS DE C2 BASEADOS EM REDES

Recentemente, a necessidade de que o EB opere de forma conjunta com as demais FA tem sido crescente. Nesse sentido, os planejamentos para o preparo e para o emprego contemplam a interoperabilidade das forças empregadas nas operações, sejam elas singulares ou conjuntas. (BRASIL, 2015)

Na interoperabilidade técnica, verifica-se a necessidade de se buscar a partir da ligação física ou da conectividade, contemplando o estabelecimento de protocolos de comunicações e a padronização de modelos de intercâmbio de dados, até se atingir a interoperabilidade da informação, com o objetivo de se obter a consciência situacional. (BRASIL, 2015)

Nesse contexto, a utilização dos mesmos protocolos de comunicação é de extrema importância para atingirmos esse nível de interoperabilidade. O MTO traz essa combinação de equipamentos que integra os Batalhões e Brigadas no SC2Ter e consequentemente está pronto para interligar-se com outras redes como a Rede Operacional de Defesa (ROD) do Ministério da Defesa (MD).

3.4 GUERRA CENTRADA EM REDES

A Guerra Centrada em Redes enfoca o espaço de batalha como uma rede integrada e escalonada em outras redes, concorrendo para aumentar a mobilidade

das peças de manobra, a coordenação entre elas e a utilização do conhecimento mútuo.

> A GCR não mudará a essência da guerra e não substituirá a força militar em si. Entretanto, propicia a esta ganhos reais em operacionalidade. Entre os benefícios trazidos pela GCR podem ser mencionados:
> a) a obtenção e o compartilhamento da consciência situacional;
> b) o incremento do poder relativo de combate em relação ao oponente;
> c) o aumento da rapidez nas decisões – e a consequente aceleração do ciclo de C2 e do ritmo das operações;
> d) a maior precisão das armas e a maior letalidade dos ataques;
> e) a agilidade na identificação de alvos;
> f) a maior proteção à Força; e
> g) a sincronização das ações. (BRASIL, 2015, p. 2-10).

Segundo Gomes, Cordeiro e Pinheiro (2016), o grande problema do crescimento de uma Rede de C2 é que as interações aumentam e, por conseguinte, mais vulnerável o sistema de C2 e por conseguinte as informações relevantes trafegam. Sendo assim, cresce de importância a proteção das informações e fontes de informação de uma variedade de ataques que podem ocorrer e prejudicar a eficiência dos sistemas de C2.

3.5 GUERRA CIBERNÉTICA

Guerra Cibernética (G Ciber), segundo o manual EB70-MC-10.232, 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. (BRASIL, 2017)

Para atacar uma rede, geralmente, o atacante utiliza-se de uma sequência lógica, que vai desde a coleta dos dados, passando pelas ações ofensivas, até a limpeza dos rastros que porventura tenha deixado.

Para se proteger dessas ações, torna-se necessário conhecer profundamente tanto o ataque como a filosofia dos atacantes, pois, desta forma, será possível escolher a melhor contramedida a ser empregada. (Gomes, Cordeiro e Pinheiro 2016)

A Guerra Cibernética é dividida em três atividades, sendo a exploração, ataque e proteção cibernética. (BRASIL, 2017)

A exploração cibernética consiste em ações de busca ou coleta nas redes de dados ou sistemas do inimigo, a fim de obter informações relevantes que podem ser empregadas em proveito da inteligência ou podem servir de subsídio para o planejamento de um ataque cibernético propriamente dito.

O Ataque Cibernético é mais agressivo e, por intermédio dele, o atacante conseguirá derrubar ou corromper total ou parcialmente redes de dados e sistemas do oponente, danificar equipamentos e dispositivos ou destruir bancos de dados e informações relevantes, podendo para isso, fazer ou não uso de técnicas de invasão.

Já a Proteção Cibernética visa a neutralizar o ataque e a exploração cibernética oponentes contra os dispositivos computacionais, as redes de computadores e de comunicações amigos, sendo uma atividade de caráter permanente.

3.6 O MÓDULO DE TELEMÁTICA OPERACIONAL (MTO)

O MTO possibilita as comunicações de dados, vídeo e voz através de rádio transmissão. Utiliza um conjunto de equipamentos integrados que fornecem um sistema flexível e móvel de comunicação tática (HARRIS, 2014).

O Módulo de Telemática Operacional (figura 4) integra diversos sistemas que dão ao usuário variados meios de comunicação. O sistema possibilita às comunicações militares via rádio integração à rede pública de telefonia fixa ou celular, transmissão de vídeo a dezenas de quilômetros, acesso à internet a até 100 km de distância da base de operações, emprego de tecnologia VoIP e integração de qualquer cenário remoto através de sistemas de comunicação via satélite. (BRASIL, 2016, p. 5).

Os elementos que compõe o MTO são:

> Ponto de Acesso AirgGuard: O ponto de acesso AirgGuard tem por finalidade integrar os dispositivos móveis, tais como smartphones e tablets, a rede MTO, sendo compatível com os padrões IEEE 802.11 a/b/g.
> Rádio RF 7800W-OU500: É utilizado para a extensão de Redes Locais (LAN) de longas distâncias (WAN). É o enlace principal entre as viaturas do MTO e destas com o escalão superior.
> Rádio RF 7800M-MP: O rádio RF 7800M-MP é um dos rádios da família Falcon III, da Harris Corporation. Este equipamento, oferece serviços de voz e dados seguros de alta velocidade e em movimento.
> Rádio RF 7800V-HH: é um rádio tático portátil , que permite a transmissão simultânea de voz e dados, com largura de banda de até 192 kbps, integrado a uma rede IP.
> RoteadorCISCO 2921: é um roteador da família 2900 e é o chamado de Roteador de Serviços Interligados (ISR), baseado em serviço de multimídia, sua função é integrar dados, vídeo e voz em um único dispositivo com flexibilidade e escalabilidade. (BRASIL, 2016, p. 13).

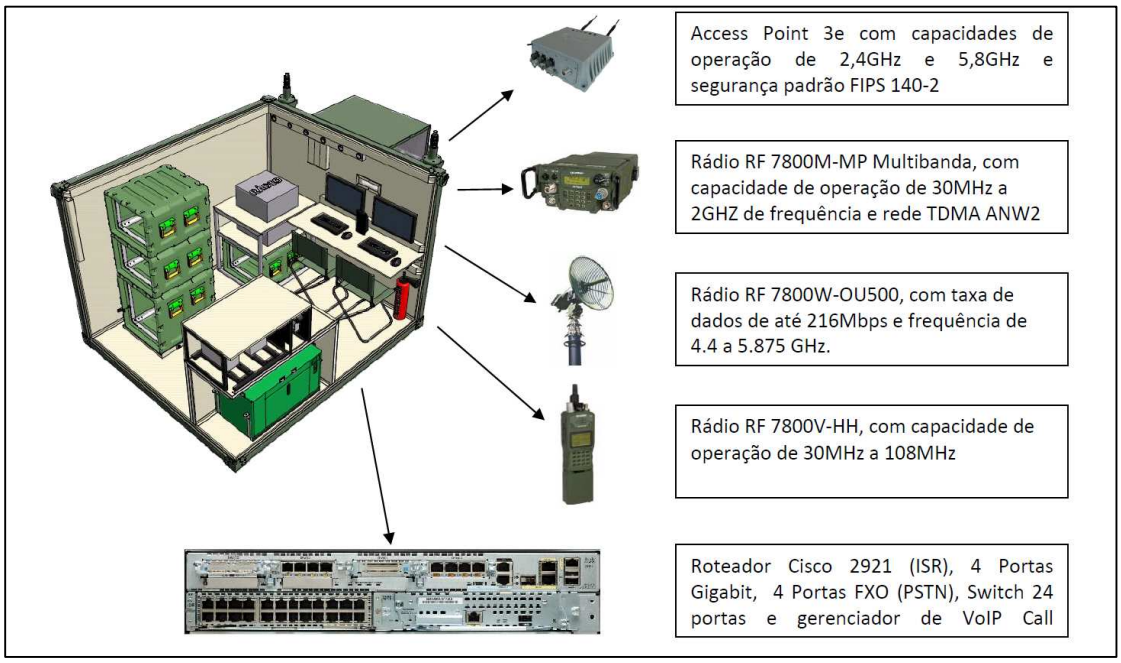

Figura 4- Elementos que compõe o MTO.Fonte: Brasil (2016).

Além dos componentes citados por Brasil (2016), o MTO possui um telefone VoIP CISCO 7942 que “permite implantar uma comunicação com facilidade e flexibilidade de voz” (BRASIL, 2016). Todo o sistema VoIP é gerenciado pelo roteador CISCO 2921. O roteador CISCO 2921 possui também um módulo de switch integrado com a finalidade de conectar os dispositivos finais dos usuários como laptop, impressoras, equipamento de vídeo conferência e o telefone VoIP CISCO 7942, para que todos os usuários utilizem os serviços de comunicação e comando e controle.

O MTO é um material de emprego militar (MEM) para roteamento de dados, que possibilita que os diversos usuários do Sistema de Comunicações Táticas (SISTAC) se conectem a qualquer outro usuário do SC²FTer. (BRASIL, 2021).

3.7 O MTO NO SISTEMA DE COMUNICAÇÕES TÁTICAS

O Sistema Tático de Comunicações (SISTAC) é o conjunto de meios de comunicações empregados por tropas em operações, utilizando-se de pessoal e de material orgânicos, destinados a apoiar as necessidades de C2 do escalão considerado. O SISTAC é subdividido em Sistema de Comunicações de Área (SCA) e Sistema de Comunicações de Comando (SCC).

O SCA está concebido para atender desde o escalão Corpo de Exército, se a situação permitir, até o PC da U/SU independente e te como finalidade prover ligações

automatizadas de grande capacidade e resiliência. Sistema de concepção nodal e deve abranger toda a zona de ação (Z Aç), permitindo que qualquer elemento possa se integrar ao sistema de comunicações do escalão considerado, desde que esteja na área de cobertura, haja compatibilidade técnica, sistêmica e operacional e que possua permissão de acesso à malha nodal.

O SISTAC possui diversas infraestruturas de comunicações, um deles é o Nó de Acesso (NA) que é definido por Brasil como: centros de comunicações que proveem a interface dos PC dos diversos escalões táticos com a malha nodal (Figura 5). Os NA, são compostos por equipamentos que permitem o estabelecimento de enlace micro-ondas e multibanda, bem como equipamentos de VFH, HF, satelitais e ERB do SAM, além de outros. (BRASIL, 2021)

O MTO é um NA que possibilita o PC ingressar no SCA e usufruir de todos os serviços e sistemas de C2 do SC2Fter. Devido a quantidade de informações sigilosas que trafegam no MTO, Brasil (2021) diz que no SISTAC, todos os meios de comunicações eletrônicos, com tráfego de dados, devem estar conectados ao Módulo de Proteção Cibernética (MPC) que se constitui em um servidor com diversos serviços embarcados, como softwares de firewall e de detecção de vírus, *trojans* e *malwares*. (BRASIL, 2021)

Cabe destacar, que a grande maioria das Unidades de Comunicações já possuem o MTO que elevam as capacidades das Grandes Unidades nas Comunicações e C2.

Atualmente, o MTO não possui o MPC e os seus equipamentos não estão configurados para proteger-se frentes aos ataques cibernéticos.

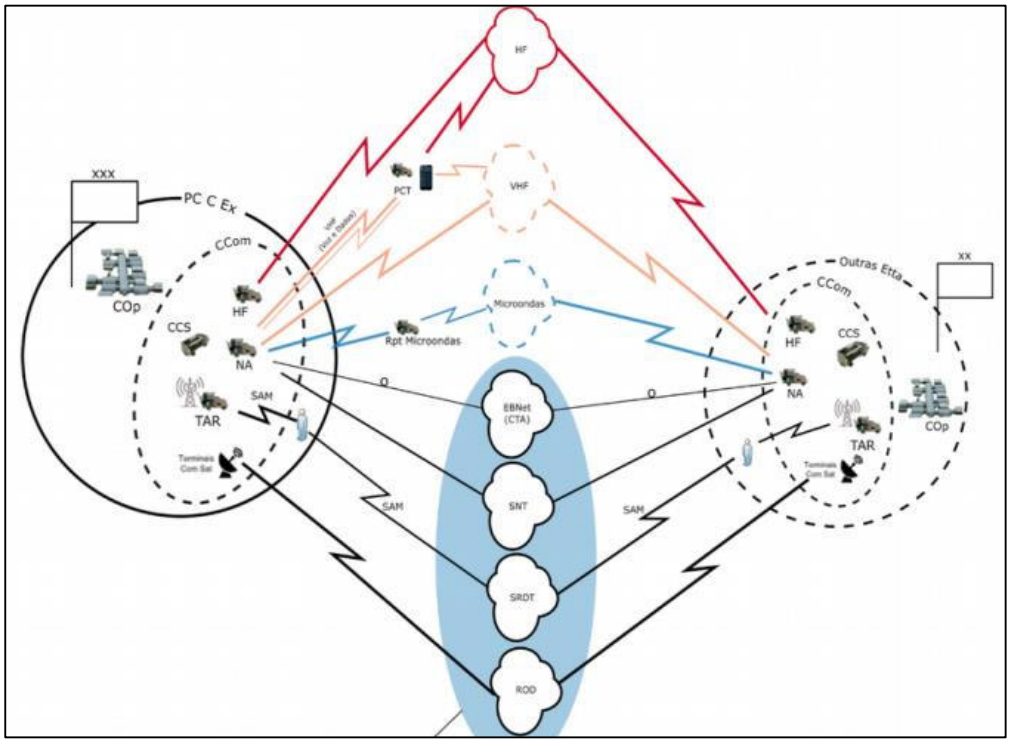

Figura 5- Desdobramento do SC2FTer Fonte: Brasil (2021).

4. VULNERABILIDADES EXISTENTES NO MTO

Segundo Carvalho (2018), por meio de testes de exploração cibernética realizados no switch e no roteador do MTO foram encontradas vulnerabilidades nos serviços e protocolos de redes disponíveis. Carvalho realizou sete ataques cibernéticos que serão listados os resultados abaixo.

4.1 ATAQUE DE *DoS CDP*

O primeiro ataque foi o de negação de serviço (*DoS*) do roteador por meio da exploração do protocolo Cisco Discovery Protocol (*CDP*). Este protocolo de camada 2 tem por objetivo de difundir informações da rede para todos os dispositivos conectados a fim de “facilitar a administração da rede para o gerente”. Nesse contexto, após o ataque, onde o invasor enviou milhares de pacotes *CDP* ao switch, ocorreu a diminuição da capacidade operativa da rede chegando ao ponto de inviabilizar a comunicação dos dispositivos.

4.2 ATAQUE DE PRIVAÇÃO DO *DHCP*

O segundo ataque foi o de privação do servidor *DHCP*. O servidor *DHCP* presta um serviço primordial em uma rede de computadores de entregar e organizar os endereços IP (camada 3) de todos os dispositivos. Nesse sentido um *host* ao se conectar na rede, recebe um endereço para poder se integrar a todos os serviços disponibilizados pela rede de C2.

Nesse contexto, o invasor fez diversas requisições de *IP*, simulando diversos computadores ingressando na rede, o que ocasionou o término de endereços *IP* disponíveis no servidor. Dessa maneira, qualquer novo dispositivo conectado a rede não conseguiu receber um endereço, negando o seu acesso a rede de C2.

4.3 ATAQUE DE ESTOURO DE *BUFFER SMART INSTALL*

O terceiro ataque foi de estouro de pilha no serviço *smart install* do roteador CISCO 2921. Esse serviço que por padrão vem ativo no roteador, permitindo que qualquer outro dispositivo CISCO possa interagir tecnicamente com o roteador, por meio da porta 4786 (camada 4). O termo estouro de pilha ou *buffer*, consiste em um envio de dados pelo atacante acima do esperado pela aplicação, quando acontece o transbordamento dos dados, o aplicativo excede o uso da memória reservada pelo sistema operacional, geralmente, dando condições de acesso ao sistema pelo invasor.

Após o ataque, o agressor teve a capacidade de interceptar todo o tráfego entre os *hosts* que trafeguem pelo roteador, e ter todas as funcionalidades de administrador. Esse tipo de ataque permitiu que o atacante interrompesse ou realizasse a captura do tráfego da rede de C2, ocasionando um alto impacto na segurança da informação.

4.4 ATAQUE DE ESTOURO DE *BUFFER TELNET*

O quarto ataque realizado por Carvalho foi o de estouro de *buffer*, por meio da aplicação Telnet, ao enviar caracteres especiais não permitidos pela aplicação do roteador, ao ocasionar o travamento do roteador, negando o serviço.

4.5 ATAQUE DE *DoS STP*

O quinto ataque foi exploração dos protocolos *Spanning Tree Protocol (STP),* de camada 2. Esse protocolo tem por missão de difundir as informações da rede para todos os dispositivos a fim de facilitar a administração do gerente. Após o ataque de

inundação de pacotes ocasionou a diminuição da capacidade operativa da rede chegando ao ponto de não conseguirem prestar o serviço (negação de serviço).

4.6 ATAQUE DE *ARP SPOOFING*

O penúltimo ataque foi o de *ARP Spoofing*. O *ARP – Address Resolution Protocol*, é um protocolo utilizado para encontrar um endereço ethernet (*MAC*) a partir do endereço *IP*. O host que está procurando um *MAC* envia através de broadcast um pacote *ARP* contendo o endereço IP do host desejado e espera uma resposta com seu endereço *MAC*, que será mapeado para o respectivo endereço IP. (ORTEGA, 2022)

Esse ataque o atacante difunde informações para toda rede informando que ele é o roteador. Nesse sentido, todos os hosts conectados começam a enviar as informações para o atacante. Esse tipo de ataque poderá causar danos ao C2, como o desvio de tráfego, captura de informações importantes como lista de usuários, senhas, fotos, vídeos e documentos na rede, acesso a outros equipamentos diretamente conectados ao *switch*.

4.7 ATAQUE DE FORÇA BRUTA

O último ataque foi de força bruta nos serviços *Telnet* e *SSH*. Esse ataque tem por finalidade de tentar adivinhar a senha do administrador, por meio de tentativas e erros. Nesse contexto, foi utilizado um dicionário de senhas com milhões de combinações de senhas. Caso a senha do administrador seja de baixa complexidade, provavelmente o invasor terá acesso como administrador do roteador.

4.8 RESUMO DOS ATAQUES E IMPACTOS DE C2

A seguir, na tabela 1, será resumido as combinações dos ataques realizados, bem como seus impactos de C2 no roteador do MTO.

Tabela 1 - Ataques e impactos de C2 no MTO

Ataque	**Impactos de C2**
Inundação *CDP*	Negação de Serviço
Privação *DHCP*	Negação de Serviço para novos usuários
Estouro de *Buffer Smart Install*	Controle do switch e roteador
Estouro de *Buffer Telnet*	Negação de Serviço

Ataque de *STP*	Negação de Serviço
Arp Spoofing	Acesso ao switch/roteador
Ataque de Força Bruta	Controle do switch e do roteador

Fonte: Carvalho (2018)

5. PROTEÇÃO CIBERNÉTICA DO MTO

Quando o assunto é proteção em rede de dados, a primeira consideração a se reconhecer é que não há nenhuma medida que proporcione 100% de eficácia. O equilíbrio adequado entre operação e segurança torna-se uma tarefa difícil nos complexos e modernos sistemas.

Segundo Gomes, Cordeiro e Pinheiro (2016), para se atingir a proteção de sistemas baseados em redes de dados, inicialmente, três verbos são fundamentais no planejamento de contramedidas: prevenir, detectar e responder. Desta forma, todo e qualquer plano de resposta a ataques cibernéticos deve conter medidas preventivas, que incluem ações de prevenção e detecção de vulnerabilidades e medidas repressivas, que são as respostas propriamente ditas aos incidentes.

Todos os ataques cibernéticos realizados no capítulo anterior foram estudados a fim de mitigar as vulnerabilidades do MTO. Nesse sentido, as medidas técnicas de prevenção desses ataques serão explicadas nas seções abaixo.

5.1 PROTEÇÃO DO ATAQUE DE *DoS CDP*

Esse ataque pode ser mitigado, desabilitando esse protocolo nas interfaces ou no equipamento por meio do comando no *cdp enable* ou no *cdp run*. A desabilitação desse protocolo não impactará no seu funcionamento, uma vez que o CDP tem como objetivo na propagação de informações para outros equipamentos. Dessa maneira o *switch* não irá mais propagar mensagens *CDP* e não estará mais vulnerável a esse tipo de ataque.

5.2 PROTEÇÃO DO ATAQUE DE PRIVAÇÃO DO *DHCP*

O *DHCP Snooping* é um recurso de segurança de camada 2, que age filtrando mensagens DHCP não confiáveis/inválidas, e para isso constrói e mantém o DHCP *Snooping Binding Database* (ou DHCP Snooping Binding Table). Ele funciona como um *firewall* entre as portas confiáveis (onde estão conectados os servidores DHCP e portas de uplink que levam aos servidores) e não confiáveis (demais portas). (ORTEGA, 2022)

Segundo Ortega, as ações executadas pelo switch configurado com DHCP Snooping:

- Valida mensagens DHCP recebidas de fontes não confiáveis e filtra mensagens inválidas.
- Faz rate-limit de tráfego DHCP de fontes confiáveis e não confiáveis.

> - Constrói e mantém o DHCP Snooping Binding Database, que contém informações sobre hosts não confiáveis com endereços IP adquiridos via DHCP.
> - Utiliza o DHCP Snooping Binding Database para validar os pedidos subsequentes de hosts não confiáveis.
> - Descarta pacotes do tipo DHCPOFFER, DHCPACK, DHCPNAK, ou pacotes DHCPLEASEQUERY, recebidos em uma porta não confiável.
> - Descarta pacotes recebidos em uma interface não confiável se o endereço MAC de origem e o endereço de hardware do cliente DHCP não coincidem.
> - Descarta mensagens broadcast DHCPRELEASE ou DHCPDECLINE que tem um endereço MAC no DHCP Snooping Binding Database, mas as informações não coincide com a interface em que mensagem foi recebida.
> - Descarta mensagens encaminhadas por um releay agent se ela tiver um endereço de relay agent diferente de 0.0.0.0.
> - Descarta mensagens DHCP com a opção de 82 se estas forem para uma porta não confiável. (ORTEGA, 2022)

A configuração do *DHCP Snooping* é simples, bastando habilitar a funcionalidade com o comando *ip dhcp snooping* no modo de configuração global, indicar a *Virtual Local Area Network* (*VLAN)* que deverá ser inspecionada, e marcar as portas que “vão” para o *DHCP* como trust confiáveis).

5.3 PROTEÇÃO DO ATAQUE DE ESTOURO DE *BUFFER SMART INSTALL*

O serviço smart install da CISCO vem por padrão habilitado nos roteadores para facilita a instalação de outros acessórios da empresa de maneira mais simples. Essas facilidades, no entanto, facilitam a exploração dos atacantes. Assim, não existe a necessidade de permanecer com esse sérvio ativo.

Para mitigar essa vulnerabilidade, o administrador deverá desabilitá-lo com o comando *no vstack* no modo de configuração global. Assim, a porta 4786 será fechado no roteador.

5.4 PROTEÇÃO DO ATAQUE DE ESTOURO DE *BUFFER TELNET*

Telnet é um serviço criado em 1977 para propiciar a comunicação do administrador com as máquinas. Esse serviço não possui criptografia de ponta a ponta, facilitando as ações dos atacantes para ler o seu conteúdo. Dessa maneira o Telnet não é aconselhável de utilizar devido a sua falta de segurança.

O serviço *SSH,* criado em 1995, tem a mesma funcionalidade do *Telnet* acrescido de criptografia ponta a ponta. Assim, deverá ser desabilitado o *Telnet* no roteador com o comando **transport input ssh** no modo de configuração de linha vty. Dessa forma, a porta 21 será fechada e não haverá mais possibilidade de realizar o ataque de estouro de buffer via Telnet.

5.5 PROTEÇÃO DO ATAQUE DE *DoS STP*

Os *switches* da infraestrutura de uma rede se comunicam entre si através da troca de quadros denominados *BPDUs (Bridge Protocol Data Units),* permitindo que, através da lógica do protocolo *STP,* todos os *switches* conheçam a topologia da ligação entre eles.

O ataque de *DoS STP* faz com que o atacante realize a manipulação dos quadros BPDUs, alterando a topologia constantemente dos switches até que eles travem.

Para mitigar esse ataque deverá ser ativado o recurso de Root Guard e BPDU Guard no switch do MTO em cada porta com o comando *spanning-tree guard root e spanning-tree portfast* no modo de configuração de interface. Essa ação não haverá impactos no funcionamento do roteador, tendo em vista que esse recurso aumenta apenas a segurança desse protocolo.

5.6 PROTEÇÃO DO ATAQUE DE *ARP SPOOFING*

Para mitigar esse ataque, o administrador deverá ativar o recurso de segurança em cada porta do switch com o comando *switchport port-security* em todas as interfaces a serem protegidas. Essa recurso garantirá uma melhor proteção cibernética nas portas conectadas ao usuário, uma vez que tenha uma atividade suspeita, o *switch* irá informar e poderá, dependendo da configuração, desativar a porta para garantir a integridade da rede.

5.7 PROTEÇÃO DO ATAQUE DE FORÇA BRUTA

As diversas tentativas de acesso ao roteador poderão permitir em algum momento o acesso do invasor aos recursos de administração. Dessa maneira para mitigar esse ataque é necessário limitar as tentativas de login. Para isso, deverá ser inserido o comando *login block-for 360 attempts 2 within 10*, o que deve bloquear as tentativas de login por 360 segundos, caso as senhas incorretas tenham sido inseridas duas vezes em até 10 segundos.

5.8 RESUMO DAS AÇÕES DE PROTEÇÃO CIBERNÉTICA

A seguir, na tabela 2, serão resumidas as combinações dos ataques cibernéticos com as ações para sua proteção.

Tabela 2 – Resumo dos ataques e proteção cibernética

Ataque cibernético	**Ação para proteção cibernética**
Negação de serviço do *CDP*	Desabilitar o serviço nas interfaces.
Ataque de privação do *DHCP*	Habilitar o recurso *DHCP Snooping.*
Estouro de *buffer smart install*	Desabilitar o serviço.
Estouro de *buffer* do Telnet	Desabilitar o recurso.
Negação de serviço do STP	Habilitar o *recurso Root Guard e BPDU Guard.*
ARP *Spoofing*	Habilitar o recurso *Port Security* nas interfaces.
Força bruta	Habilitar o recurso contra o ataque de força bruta.

Fonte: Próprio autor (2022)

6. CONCLUSÃO

Este trabalho teve por finalidade realizar uma proposta de proteção cibernética para o MTO. Nesse sentido, o objeto de análise é muito importante para o C2 da F Ter devido as valiosas informações trafegadas nesse equipamento durante o seu emprego.

Cada vez mais, os sistemas de C2 estão mais conectados em rede, onde a G Ciber se mostra com um diferencial para o aumento do poder de combate. Suas ações podem interromper os sistemas de C2 e comprometer as tomadas de decisão precisas e oportunas. Consequentemente, a proteção cibernética dos ativos da informação é primordial para evitar a quebra da continuidade das comunicações.

Nesse ínterim, como visto no capítulo 3, o MTO corresponde a soma de diversos equipamentos instalados em uma viatura para proporcionar Comunicações e C2 para os elementos dos diversos escalões empregados. Contudo esse material encontra-se apenas no Exército Brasileiro. Assim, essa particularidade se tornou uma limitação desse estudo, devido a pequena quantidade de trabalhos elaborados sobre o tema.

Dessa maneira, no capítulo 4, foi imprescindível o trabalho de Carvalho, 2018 que ao realizar os ataques cibernéticos no MTO pode demonstrar suas vulnerabilidades, que puderam ser estudadas e mitigadas com o presente trabalho, contribuindo para a realização da proposta de proteção cibernética.

No capítulo 5, pode-se identificar uma forma técnica de se proteger contra os ataques, como os ataques de negação de serviço do *CDP*, ataque de estouro de *buffer* de *smart install* e de estouro de *buffer* do serviço *telnet* que de maneira simples foram corrigidos.

Ainda no capítulo 5, o ataque de privação do servidor *DHCP*, o ataque de negação do serviço do *STP*, o ataque de ARP *spoofing* e o ataque de força buta, necessitaram de outros mecanismos de proteção, como a ativação de recursos de segurança presentes no roteador que por padrão estavam desabilitados.

Assim, conclui-se que a proposta de proteção cibernética do MTO do presente trabalho foi efetivada pelo empregado de medidas de segurança que já existem no próprio equipamento, necessitando apenas de refinar suas configurações para atingir o objetivo desejado.

Destarte, a tabela 2 que consta no capítulo 5 desse trabalho, na qual resume as ações que o administrador do MTO deverá realizar para solucionar o problema em questão, o que poderá de maneira técnica corrigir a vulnerabilidade sem comprometer o funcionamento do equipamento.

Apesar dessa posposta não necessitar de mecanismos externos de segurança, como outros equipamentos para sua eventual proteção, como sugestão de trabalhos futuros seria o aprimoramento da proteção do MTO no prisma de segurança em camadas. Esse termo consiste na disposição de diversas etapas de proteção à operacionalidade de uma rede ou sistema, de modo a blindar seus ativos e informações mais sensíveis contra os ataques cibernéticos. Dessa forma, trata-se de uma metodologia que reforça as fronteiras digitais com vários muros de sustentação, aqui caracterizados como firewalls e recursos de criptografia.

Nesse sentido, enfatizando o MTO como um dos elementos que fazem parte do SC2FTer como implementações de novos recursos de segurança sugere-se o estudo de algumas tecnologias: protocolos de criptografia nas camadas 3 e 4 do modelo OSI como o IPSec e SSL/TLS, respectivamente, para garantir uma comunicação segura nas camadas mais baixas, garantindo da integridade e confidencialidade na informação; *IDS* (Sistema de Detecção de Intrusão) e *IPS* (Sistema de Prevenção de Intrusão), que tem como objetivo de detectar e impedir o tráfico malicioso na rede e Firewall do tipo *Next Generation* ou de próxima geração que fazem um gerenciamento unificado das ameaças na rede, o que diferencia dos *firewalls* convencionais.

Além disso para aprimorar a proteção cibernética do MTO, deverá ser estudado outras formas para fortalecer a segurança em camadas como: a proteção humana, como a valiosa preparação das pessoas para enfrentarem esse problema e evitarem de cair em métodos de engenharia social, por exemplo; A proteção física dos equipamentos como a inserção de câmeras, travas de segurança e alarmas para prevenir de um acesso não autorizado e comprometer o equipamento fisicamente; A segurança dos dispositivos finais, ou conhecidos também com *end point,* que tem por missão de proteger os dispositivos e programas executados pelos usuários finais que podem servir como uma brecha para entrada de invasores nos sistemas, como criptografar dados locais, controle dos aplicativos instalados, manter o sistema sempre atualizado e analisar com regularidade os arquivos em busca de algum malware.

A Escola de Comunicações criou em .2021 o Curso de Proteção Cibernética para oficiais e sargentos e com essa medida, os futuros administradores e operadores do MTO sairão com essa competência e poderão assegurar o uso eficiente das redes de computadores.

Ainda, como sugestão de melhorias, sugiro a criação de um capítulo no caderno de instrução do operador do Módulo de Telemática Operacional sobre a aplicação dessas medidas de proteção cibernéticas para evitar esses tipos de ataques e que seja disseminado para os administradores e operadores do MTO, ou de um Manual de Proteção Cibernética, onde será explicado os principais conceitos e formas de aplicação dessa atividade na função de combate proteção.

Dessa forma, o objetivo geral de propor medidas de proteção cibernéticas para o MTO, bem como todos os objetivos específicos deste trabalho foram alcançados com sucesso. Ressalta-se a necessidade de prosseguimento dos estudos sobre essa temática para a evolução dos aspectos técnicos.

REFERÊNCIAS

ARCHANGELO, Marco Antonio Altruda. **Um estudo acerca da relação entre a defesa cibernética e a função de combate logística**. 2019.

ARMY CYBER. **About army cyber command: the army's frontline of cyber warfare.** 2019. Disponível em: <https://www.goarmy.com/army-cyber/about-armycyber-command.html>. Acesso em 05 de junho de 2021.

BLACKBERRY. **Relatório de Ameaças 2021.** 2021. Disponível em: <https://www.blackberry.com/us/en/pdfviewer?file=/content/dam/blackberry-com/asset/enterprise/pdf/direct/report-bb-2021-threat-report-pt.pdf>. Acesso em 06 de junho de 2021.

BRASIL. **Estratégia Nacional de Defesa.** Brasília. 2020. Disponível em: <www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm>. Acesso em: 05 de junho de 2021.

_____.**Livro Branco de Defesa Nacional**. Brasília: 2012, 282p. Disponível em:< http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf > Acesso em: 10 abr.2022.

_____. Ministério da Defesa. **MD31-M-08 Doutrina Militar de Defesa Cibernética.** 1. ed. Brasília, DF, 2014.

_____. Exército. Estado-Maior do Exército. **EB20-MC-10.205 Comando e Controle.** 1. ed. Brasília, DF, 2015.

_____. Ministério da Defesa**. Caderno de Instrução do Operador do Módulo de Telemática Operacional**. EB70-CI-11.406. Brasília, DF, 2016.

_____. Exército. Comando de Operações Terrestres. **EB70-MC-10.232 Guerra Cibernética.** 1. ed. Brasília, DF, 2017.

_____. Exército. Comando de Operações Terrestres. **Nota Doutrinária Nr 04/2021 Sistema de Comando e Controle da Força Terrestre**. Brasília, DF, 2021.

_____. Ministério da Defesa. **Cenários de Defesa 2020 – 2039:** sumário executivo. Brasília, DF, 2017.

_____. Exército. Comando de Operações Terrestres. **EB70-MC-10.225 Força Terrestre Componente.** 1. ed. Brasília, DF, 2019.

_____. **Política Nacional de Defesa.** Minuta. Brasília. 2020. Disponível em: <https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf>. Acesso em 10 de abril de 2021.

CARDOSO, Luiz Henrique Filadelfo; ZIGUNOW, Lucas Maurício Alves. **Implementação de testes de invasão em apoio à proteção cibernética de redes e sistemas de interesse da Defesa**. O Comunicante, v. 9, n. 1, p. 23-32, 2019.

CARVALHO, Victor. **Impactos de ataques cibernéticos em redes operacionais de comando e controle no switch do Módulo de Telemática Operacional**. 2018. TCC (Especialização) – Curso de Guerra Cibernética, Centro de Instrução de Guerra Eletrônica, Brasília, 2018.

DE LIMA, Walbery Nogueira et al. **Atuação colaborativa da Defesa Cibernética na proteção de infraestruturas críticas de interesse para a Defesa Nacional**. Data & Hertz, v. 1, n. 1 jan./Dez, p. 52-59, 2020.

DOS SANTOS, Marcel. **O emprego da proteção cibernética para ampliar a segurança nos Postos de Comando da Força Terrestre Componente**. 2021. TCC (Especialização) – Curso de Comando e Estado-Maior do Exército, Escola de Comando e Estado-Maior do Exército. Rio de Janeiro. 2021.

FELIPPETTI, Marco. **CCNA 5.0 Guia completo de estudo**. São Paulo. Visual Books, 2014.

GOMES, Mauro Guedes Ferreira Mosqueira; CORDEIRO, Sandro Silva; PINHEIRO, Wallace Anacleto. **A Guerra Cibernética: exploração, ataque e proteção cibernética no contexto dos sistemas de Comando e Controle (C2)**. Rio de Janeiro: RMCT, v. 33, n. 2, 2016.

HARRIS. **Treinamento Sistema MTO**. Harris Corporation. Brasília-DF, 2014.

HOSANG, Alexandre. **Política Nacional de Segurança Cibernética: uma necessidade para o Brasil**. Escola Superior De Guerra, Rio De Janeiro, 2011.

VIANNA, Eduardo Wallier; DE SOUSA, Renato Tarciso Barbosa. **Ciber Proteção: a segurança dos sistemas de informação no espaço cibernético**. RICI Revista Ibero-Americana de Ciência da Informação, Brasília, v. 10, n. 1, p. 110-131, 2017.

ODOM, Wendell. **Guia Oficial de Certificação Cisco CCNA Routing and Switching ICND2 200-101**. São Paulo: Alta Books, 2006.

OLIVEIRA, Marcelo Mendes. **A defesa cibernética, o Exército Brasileiro e a gestão de projetos**. 2021.

ORTEGA, André. **DHCP Snooping: Protegendo sua rede contra servidores DHCP falsos**. Brainwork, 2022. Disponível em: < https://brainwork.com.br/2015/04/29/dhcp-

snooping-protegendo-sua-rede-contra-servidores-dhcp-falsos/ >. Acesso em: 14, agosto e 2022.

PRADO, Felipe. **Brasil foi 5º país com mais ataques cibernéticos no ano: relembre os principais**. Disponível em: https://www.istoedinheiro.com.br/brasil-foi-5o-pais-com-mais-ataques-ciberneticos-no-ano-relembre-os-principais/Acesso em 10 de abril de 2022.

PRADO, William. Mini Curso de Redes. Disponível em: https://minicursoderedes.wordpress.com/2009/12/04/modelo-osi/. Acesso em 14 de julho de 2022.

SÊMOLA, M. **Gestão de segurança da informação**. São Paulo. Campus, 2003.

VIANNA, Eduardo Wallier. **Segurança da informação digital: proposta de modelo para a Ciber Proteção nacional**. 2019.

TANENBAUM, A. S. **Redes de computadores**. São Paulo: Campus, 2003.