2º SARGENTO LONGHI
Praça da 12ª Companhia de Comunicações Leve (Aeromóvel).

A NECESSIDADE DE REDE EXCLUSIVA DE DADOS NO EXÉRCITO BRASILEIRO

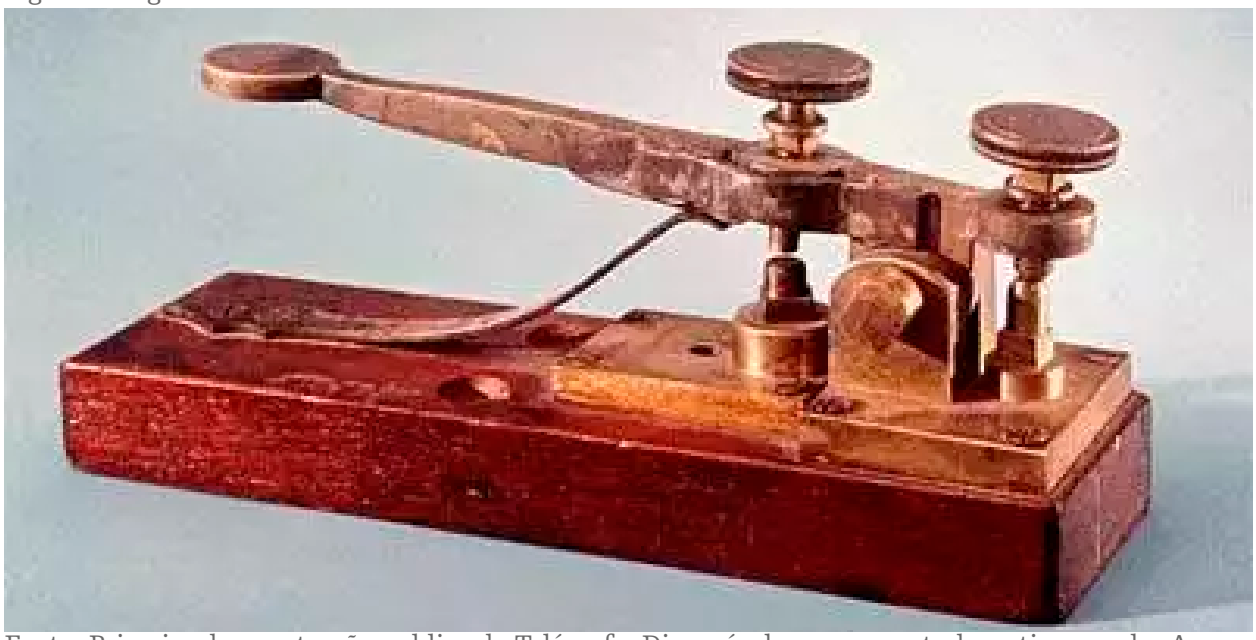
A necessidade do ser humano em se comunicar e transmitir informações fez com que nossos antepassados criassem meios de comunicações que utilizamos até hoje, como a escrita, com registros datados de 15.000 A.C. Porém, nas últimas décadas, as transformações digitais aliadas à evolução dos meios de comunicações vêm tendo saltos tecnológicos muito rápidos, o que acaba tornando seus equipamentos obsoletos em curto espaço de tempo.

Para se ter uma ideia da velocidade de desenvolvimento, uma das primeiras invenções tecnológicas para se comunicar foi o telégrafo, criado pelo francês Claude Chappe em 1792, que se disseminou rapidamente pelo império de Napoleão. Em 1876, Alexandre Graham Bell criou o telefone, paralelamente, surgiu a comunicação por meio da radiotransmissão, que teve seu auge durante a Primeira Guerra Mundial. A ligação do Brasil com a Europa através de cabos telegráficos submarinos ocorreu em 1874 e houve a primeira transmissão oficial de rádio, no Brasil, em 1922.

Um ponto importante da história e que está ligada diretamente com o desenvolvimento das comunicações, no Brasil, foram as expedições do Marechal Rondon pelos rincões do país, lançando linhas telegráficas e interligando regiões afastadas, como as do Mato Grosso aos grandes centros. Essas expedições ocorreram de 1892 até 1915, que consagraram Rondon como herói nacional e um exemplo a ser seguido.

Desde o início do século XX, a televisão foi sendo desenvolvida e a primeira transmissão com público foi feita pelo engenheiro britânico John Logie Baird, em 1926, há cerca de 97 anos. Desde então, o rumo das comunicações foi sendo alterado drasticamente e um dos maiores feitos nesse ramo foi com o desenvolvimento do primeiro computador mecânico, em 1890, pelo norte-americano Hermann Hollerith, e da primeira geração de computadores modernos que utilizavam válvulas, criado em 1943, pelo inglês Alan Turin. O primeiro celular surgiu em 1973, criado pelo engenheiro eletrônico Martin Cooper.

Fig 1 – Telégrafo de Morse.



Fonte: Primeira demonstração publica do Telégrafo. Disponível em www.estudopratico.com.br. Acesso em: 27 fev. 2023.

Fig 2 – Primeiro celular criado.

Fonte: Conheça a história do celular e sua evolução com o passar dos anos. Disponível em: www.techtudo.com.br. Acesso em: 27 fev. 2023.

Do aparecimento do telégrafo até a criação do primeiro celular se passaram 151 anos. Essas invenções foram essenciais para toda a história da humanidade, sendo inclusive decisivas em algumas guerras. Por isso, muitos países tentam aprimorar cada vez mais as suas comunicações e as suas tecnologias, uma vez que isso tem sido essencial para decidir doutrinas militares e decisivo em conflitos armados.

Com todo esse avanço tecnológico, a segurança também precisou evoluir, uma vez que manter a confidencialidade, a autenticidade, a integridade e a disponibilidade dos meios de comunicações, tratando-se de tema sensível, é essencial. O telégrafo sofreu com isso, pois ao contrário das cartas, que para conseguir interceptar, sem deixar vestígios, necessitava-se de muita habilidade, os cabos telegráficos ficavam expostos, desta forma uma interceptação clandestina era muito mais fácil. Foi devida à necessidade de se criar mecanismo para evitar esse tipo de invasão que foram sendo desenvolvidas ferramentas de segurança, como a criptografia.

Nos tempos atuais, quem invade os meios de comunicação de forma ilegal é conhecido como crackers [1]. Os danos que eles podem causar aos sistemas de segurança, por exemplo, são imensos. Quase tudo hoje é conectado por meio da rede mundial de computadores e as Forças Armadas não fogem a essa regra. Seus sistemas de armas, de comunicações, de logística e de estratégia estão, direta ou indiretamente, ligados a uma rede de dados, muitas vezes conectados à internet.

Em 2015, um grupo invadiu o sistema do Exército Brasileiro (EB) e vazou dados privados de militares. Os sistemas de defesa não foram invadidos, porém algumas informações pessoais dos militares foram expostas na internet. Após a entrada em vigor da Lei 13.709/2020, também chamada de Lei Geral de Proteção de Dados (LGPD), em 2020, além de cuidar de sistemas internos de defesa, o EB precisou cuidar também dos dados pessoais dos militares. Para isso, a segurança na rede interna deve estar constantemente sendo monitorada e protegida.

Investir em segurança de dados não é apenas criar procedimentos físicos ou lógicos. Há, portanto, a necessidade de capacitar e treinar os usuários e principalmente quem trabalha diretamente com esses ativos.

Uma rede de dados que compartilha dados privados, apesar de toda segurança implementada, corre riscos de ser invadida. Basta apenas uma vulnerabilidade explorada em um ponto de acesso à rede e todo o sistema pode ser comprometido. Por isso investir em rede exclusiva de transmissão de dados é essencial para manter a segurança das comunicações no âmbito do EB.

Na 4ª Brigada de Cavalaria Mecanizada (4ª Bda C Mec) foi implantada a fase piloto do Sistema Integrado de Monitoramento da Fronteira (SISFRON), uma rede exclusiva do Exército chamada de Infovia [2], que possibilita conectar os sensores às organizações militares (OM) das grandes unidades por intermédio de cabos de

fibra óptica ou por torres de transmissão, permitindo, assim, manter controle maior de tudo que é transmitido sem utilizar sistemas de terceiros para fazer essa conexão. Atualmente, o SISFRON se encontra em implantação da fase 2, abrangendo as áreas da 18ª Brigada de Infantaria de Pantanal (18ª Bda Inf Pan), Corumbá-MS e da 13ª Brigada de Infantaria Motorizada, em Cuiabá-MT.

SEGURANÇA DA INFORMAÇÃO (SEG INFO)

Segurança da informação é um conceito utilizado para se referir à proteção de dados e garantir que esses dados sejam acessados apenas pelos seus responsáveis de direito.

Atualmente, as maiores empresas do mundo são de tecnologia e têm como seu principal produto a proteção de dados de seus usuários. Empresas, como a Aphabet, dona do Google, e a Meta, dona do Facebook, investem sistematicamente em segurança da informação, com a finalidade de manter seus dados protegidos e mesmo assim é comum boatos sobre invasões e vazamento de informações sensíveis.

Antes de prosseguir, é necessário abordar conceitos que envolvem a segurança da informação e da informática como um todo. A seguir, aborda-se dois termos que costumam ser confundidos por muitos usuários que devem ser citados:

• **Internet:** é uma grande rede mundial de computadores que interliga desde computadores pessoais, como notebooks, até grande computadores. Pode utilizar para fazer essa conexão linhas comuns de telefone, linhas privadas de comunicação, cabos submarinos, canais de satélites e diversos meios de comunicação.

• **Intranet:** é uma rede de computadores semelhante à Internet, porém acessível apenas por determinada organização. No EB, existe uma intranet corporativa que é denominada de EBNet.

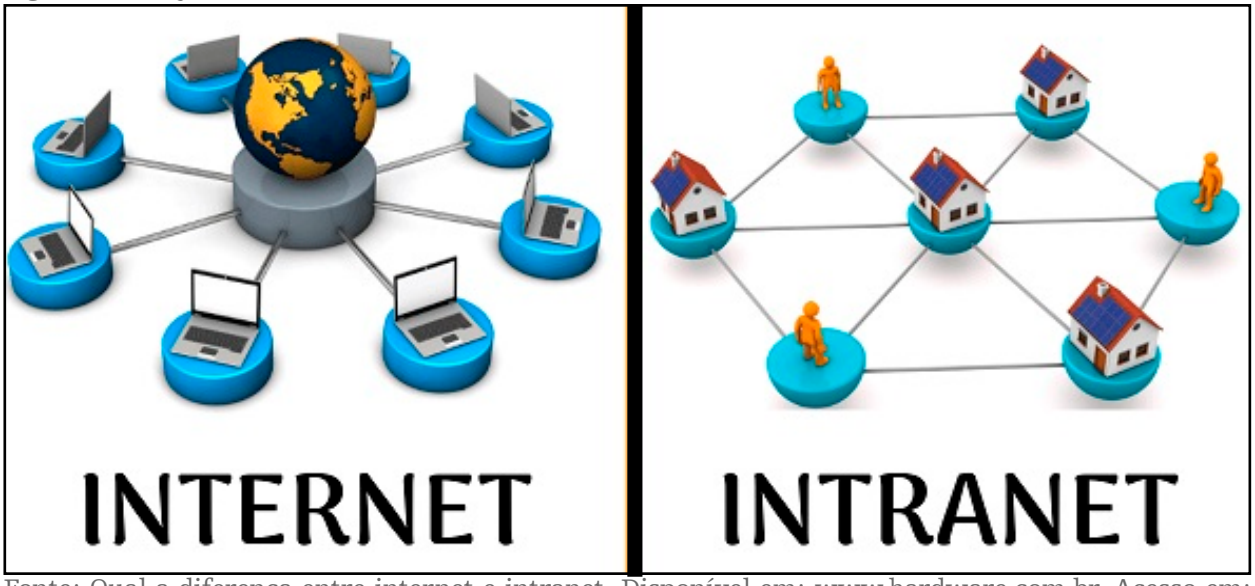
Existem várias maneiras de se garantir a segurança das informações tanto na internet quanto na intranet, sejam elas por meios físicos ou por meios lógicos (digitais). O fato da intranet ser uma rede interna torna o controle muito mais fácil, além de possibilitar a rapidez e eficácia para se identificar possíveis falhas ou tentativas de invasão. No entanto, um dos grandes problemas que todas as empresas enfrentam é justamente o que é transmitido por meio da internet.

Segundo Andrew Stuart Tanenbaum (Redes de Computadores, 4ª ed, p. 54):

> A internet não é de modo algum uma rede, mas sim um vasto conjunto de redes diferentes que utilizam certos protocolos comuns e fornecem determinados serviços comuns. É um sistema pouco usual no sentido de não ter sido planejado nem ser controlado por ninguém.

Como o controle da internet não é

Fig 3 – Ilustraçao de internet e intranet.



Fonte: Qual a diferença entre internet e intranet. Disponível em: www.hardware.com.br. Acesso em: 27 fev. 2023.

atribuído a apenas uma entidade, ela se torna muito mais insegura, pois todos têm acesso a tudo. Logo, uma vulnerabilidade em algum computador que está conectado à internet pode ser explorada por qualquer pessoa que também tenha acesso a essa grande rede.

IMPORTÂNCIA DE UMA REDE EXCLUSIVA

Como abordado no tópico anterior, a internet é uma "terra sem dono". Por isso, deve ser tratada como possível potencial de vulnerabilidade para a segurança da informação no Exército Brasileiro.

Em 2013, Edwartd Snowden revelou ao mundo que os Estados Unidos da América (EUA) praticava espionagem em diversos países, utilizando servidores de empresas, como Google, Apple e Facebook. O Brasil não escapou dessa espionagem, pois foi revelado que a então presidente do país também tinha sido alvo de espionagem.

Ataques cibernéticos também têm ganhado força nos últimos anos. Como exemplo temos, em 2015, a rede elétrica da Ucrânia que foi atingida por um ataque cibernético o que causou um apagão de curta duração, afetando cerca de 80 mil pessoas no oeste do país.

O Exército Brasileiro, cuja missão constitucional primordial é a defesa da Pátria (BRASIL, 1988), precisa aperfeiçoar seus sistemas de defesa cibernética, o que já vem acontecendo nos últimos anos. No entanto, existem algumas vulnerabilidades que podem afetar toda essa segurança.

Atualmente, OM possuem sua conexão com a internet através de provedores particulares. Os Centros de Telemática de Área (CTA) às vezes têm dificuldade em proporcionar o controle adequado para o acesso a redes externas, deixando que cada seção de informática controle esse serviço. Mesmo que os quartéis utilizem de Virtual Private Network (VPN) [3] para fazer essa conexão segura, na rede mundial de computadores não é possível garantir essa segurança. Em 2018, por exemplo, o serviço NordVPN, que prometia privacidade aos seus usuários, sofreu um ataque hacker [4], o que mostra que mesmo utilizando VPN as invasões podem ocorrer.

Segundo dados da Kaperseky Lab, o Brasil é o líder, na América Latina, quando se fala em ataques de ransomware [5], respondendo por 55% dos ataques na região. Isso só evidencia a necessidade de treinamento e capacitação dos militares que atuam direta ou indiretamente com dados sensíveis, bem como a criação e a manutenção de uma rede exclusiva.

Um jeito de tentar evitar esse tipo de invasão através da internet ou de VPNs seria a implementação de uma rede exclusiva de dados, como acontece no Comando Militar do Oeste (CMO) através da Infovia, implementada pelo Projeto do SISFRON. Com essa Infovia todos os quartéis atendidos por ela não precisam mais contratar serviços privados de internet, sendo limitado a isso apenas o CTA, por onde todo o acesso é controlado, aumentando assim a segurança da rede interna.

A infovia é formada por antenas instaladas dentro de áreas militares ou de locais públicos, quando possível, proporcionando a conexão através de transmissão via rádio ou de fibra óptica, quando a distância não é muito grande. Essa rede, ainda, permite que militares, executando treinamento nos campos de instrução, consigam ter acesso a ela, através de viaturas específicas, interligando assim não só a parte administrativa das OM como também a parte operacional.

Atualmente, o Centro Integrado de Telemática do Exército (CITEx) possui um projeto, que já está sendo implementado, o Projeto Backbone Nacional (EBGIGA), que tem como objetivo aumentar a capacidade de tráfego de dados da EBNet e evitar a dependência e os elevados custos com a contratação de provedores de comunicações privados.

Além desse sistema, por meio de cabeamento físico ou transmissões de rádio por antenas, é possível também implementar uma rede de satélite, utilizando os nacionais para poder alcançar localidades onde é inviável a utilização de outros meios, como regiões isoladas da Amazônia.

INTEROPERABILIDADE E ECONOMICIDADE

Segundo o Dicionário Online de Português, "interoperabilidade" é a "capacidade de trabalhar em conjunto que possibilita a interação entre pessoas, sistemas de operação ou organizações, buscando uma troca de informações mais eficiente e produtiva" (INTEROPERABILIDADE, 2023). A par desse conceito, a utilização de uma rede exclusiva, por meio de Infovia e do EBGIGA, poderá permitir que as outras forças armadas possam utilizar da infraestrutura para realizar suas comunicações.

Como a Infovia é um meio de transmissão de dados, a implementação de sistemas específicos da Força Área Brasileira (FAB) ou da Marinha do Brasil (MB) poderá utilizar-se dessa infraestrutura para controlar e coordenar seus sistemas, sem prejudicar o sistema do Exército, aumentando a interoperabilidade entre as forças e mantendo a segurança das comunicações.

Outra maneira para alcançar essa integração seria a utilização dessas antenas para a implementação de rádios do sistema RDS-Defesa; projeto estratégico do Ministério da Defesa, que tem como foco a criação de um sistema de rádio multibanda que possa atender às demandas das três Forças Armadas e, dessa forma, aumentar a interoperabilidade entre elas.

Além dessa possibilidade, também seria possível a utilização da infraestrutura de antenas do sistema, para a implementação de sistemas de comunicações de outros órgãos de segurança pública (OSP), como já acontece na 4ª Bda C Mec, onde em alguns locais as antenas da Infovia são utilizadas pela Secretaria de Segurança Pública para colocação de câmeras de vídeo monitoramento ou de antenas dos seus equipamentos rádio. Desse modo, a integração entre as Forças Armadas (FA) e os OSP facilitariam futuras operações conjuntas ou interagências.

Umas das vantagens da implementação de uma rede exclusiva de transmissão de dados está na economicidade, pois boa parte da tecnologia para a criação desses sistemas já existe no Brasil. Empresas nacionais poderiam desenvolver e ajudar na implementação do sistema, garantindo, assim, autonomia e o baixo custo da implementação, além de auxiliar no desenvolvimento da industria nacional, evitando gastos com contratação desse tipo de serviço por empresas estrangeiras.

CONSIDERAÇÕES FINAIS

Nos atuais conflitos armados, que acontecem pelo mundo, equipamentos, como drones e balões, são utilizados com maior frequência tanto para realizar ataques como para realizar espionagens.

Várias empresas já sofreram ataques em seus sistemas, o que causou grandes prejuízos financeiros, além de comprometer a segurança nacional, principalmente quando os ataques foram direcionados a órgãos públicos, como hospitais, usinas de energia elétrica, sistema de água ou até em sistemas de defesa militar.

Atualmente, a busca por informações privilegiadas, seja de pessoal ou de atividades militares, é essencial para determinar futuras operações ou até mesmo políticas de governo. Para manter esses dados em segurança, é importante investir em treinamento e capacitação das Forças Armadas. Cabe destacar que a LGPD prevê multas para quem não proteger corretamente os dados de seus usuários.

Uma rede exclusiva de dados, na qual se pode ter maior confiabilidade no que está sendo transmitido e maior garantia de autenticidade, será essencial para colocar o Exército Brasileiro como referência militar no trato da segurança da informação, como já acontece no setor estratégico Defesa Cibernética.

Por fim, a possibilidade de unir projetos que já existem e estão em andamento, por iniciativas de diversos setores governamentais, poderá, em futuro próximo, consolidar mudanças benéficas para a sociedade e para o Estado brasileiro, neutralizando ou evitando danos no caso de comprometimento de infraestruturas críticas e de vazamentos de informações sensíveis.

REFERÊNCIAS

RENATO, Flávio. Conheça a história do celular e sua evolução com o passar dos anos. TechTudo, 2022. Disponível em: https://www.techtudo.com.br/noticias/2022/09/conheca-a-historia-do-celular-e-sua-evolucao-com-o-passar-dos-anos.ghtml. Acesso em: 20 fev. 2023.
GADELHA, Juliana. A Evolução dos Computadores, IC UFF. Disponível em: http://www.ic.uff.br/~aconci/evolucao.html. Acesso em: 20 fev. 2023.
OS 96 ANOS DA PRIMEIRA TRNASMISSÃO DE TV NO MUNDO. Memórias Cinematográficas, 2021. Disponível em: https://www.memoriascinematograficas.com.br/
2021/02/os-95-anos-da-primeira-transmissao-de.html. Acesso em: 20 fev. 2023.
SOUZA, Rafaela. Meios de Comunicação. Mundo Educação. Disponível em : https://mundoeducacao.uol.com.br/geografia/meios-comunicacao.htm. Acesso em: 21, fevereiro de 2023.
COSTA SANTOS DIAS, Juliana. O Telégrafo, a invenção que deu início a era da informação. Kapersky. Disponível em: https://www.kaspersky.com.br/blog/telegraph-grandpa-of-internet/5431/. Acesso em: 19 fev. 2023
Hackers invadem servidores do Exército e vazam CPFs de militares. G1, 2015. Disponível em: https://g1.globo.com/tecnologia/noticia/2015/11/hackers-invadem-servidores-do-exercito-e-vazam-cpfs-de-militares.html>. Acesso em: 10 fev. 2023.
VELASCO, Ariane. O que é Segurança da Informação?. Canaltech, 2019. Disponível em: https://canaltech.com.br/seguranca/seguranca-da-informacao-o-que-e-158375/. Acesso em: 10 fev. 2023.
TANENBAUM, Andrew. Redes de Computadores – 6. ed. - Editora Bookman, 2021.
ROHR, Altieres. Serviço NordVPN, que promete 'privacidade' na internet, revela que foi vítima de ataque hacker. G1, 2019. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2019/10/22/servico-nordvpn-que-promete-privacidade-na-internet-revela-que-foi-vitima-de-ataque-hacker.ghtml. Acesso em: 10 fev. 2023
TIDY, Joe. Guerra na Ucrânia: os três ciberataques russos que as potências ocidentais mais temem. BBC, 2022. Disponível em: https://www.bbc.com/portuguese/internacional-60843427. Acesso em: 10 fev. 2023.
INTEROPERABILIDADE. In: DICIO, Dicionário Online de Português. Porto: 7Graus, 2023. Disponível em: <https://www.dicio.com.br/interoperabilidade/>. Acesso em: 10 fev 2023.

NOTAS

[1] *Crackers* são indivíduos com habilidades avançadas em computação e segurança da informação que utilizam essas habilidades de forma maliciosa para acessar sistemas de computadores, redes, softwares ou dados sem autorização. Dessa forma, *crackers* podem explorar vulnerabilidades e falhas de segurança para invadir sistemas e obter acesso não autorizado.
[2] É uma rede de comunicação, formada por cabos de fibra óptica e antenas de transmissão via rádio, que transmite voz, dados e imagens entre dispositivos nela conectados.
[3] VPN significa *Virtual Private Network* (Rede Privada Virtual) e descreve a oportunidade de estabelecer uma conexão de rede protegida ao usar redes públicas.
[4] *Hacker* é uma palavra da língua inglesa que, no âmbito da informática, designa alguém capaz de invadir dispositivos eletrônicos, redes e sistemas de computação, seja para verificar sua segurança, para aperfeiçoá-lo ou para praticar atos ilícitos.
[5] *Ransomware* é um *software* de extorsão que pode bloquear o seu computador e depois exigir um resgate para desbloqueá-lo.

SOBRE O AUTOR

O 2° Sargento de Comunicações Matheus Longhi Simal é o Adjunto da Seção de Informática da 12ª Companhia de Comunicações Leve (12ª Cia Com L), sediada em Caçapava-SP. Foi promovido à graduação de 3º Sargento, em 2013, na Escola de Sargentos das Armas (ESA). Em 2023, concluiu o Curso de Aperfeiçoamento pela Escola de Aperfeiçoamento de Sargentos das Armas, sediada em Cruz Alta-RS. Possui os cursos: Básico de Guerra Eletrônica para Sargentos, ISO 20.000 e ITIL - Melhores Práticas em Gerenciamento de Serviços de TI no SisTEx, CCNA Routing and Switching - Módulo I e Módulo II. Participou de diversas Operações na Faixa de Fronteira, Operações de Cooperação e Coordenação com Agências e com Órgãos federais e estaduais, Operações da Arma de Comunicações e de diversas Experimentações Doutrinárias do Batalhão de Comunicações e Guerra Eletrônica. Possui curso superior em Tecnólogo de Redes de Computadores pela Faculdade Campo Grande (FCG) (longhi.matheus@eb.mil.br).