MAJOR DIOGO LUIZ
Oficial de Operações do Centro de Defesa Cibernética.

A EXPLORAÇÃO E O ATAQUE CIBERNÉTICO

Muito se comenta sobre como o domínio cibernético tem se ampliado e como ele também é intrínseco aos demais domínios naturais: terra, mar, ar e espaço. O fluxo constante de dados pelo ciberespaço faz parte do cotidiano da sociedade brasileira, que está cada dia mais conectada. Uma nova fronteira, até então inexistente, foi aberta, sendo imperativo guarnecê-la. Temas ligados à atuação estatal e não estatal nesse ambiente têm sido tratados por uma ampla gama de entidades e assuntos, como soberania, legalidade e legitimidade das ações cibernéticas, estando na ordem do dia de instituições e indivíduos.

As Forças Armadas, acompanhando a evolução dos tempos, têm buscado garantir que o poder nacional brasileiro seja também manifestado no domínio cibernético. Esse ambiente possui particularidades específicas e necessita de capacidades e competências peculiares para sua efetiva utilização no âmbito de operações militares.

A Doutrina de Operações Conjuntas, referência doutrinária brasileira mais atual sobre a Guerra Cibernética, divide a Capacidade Cibernética em três capacidades operativas [1]: proteção cibernética, exploração cibernética e ataque cibernético.

A proteção cibernética é o conceito que causa menos dificuldade de compreensão. Ela representa o escudo que garante o funcionamento dos dispositivos computacionais do teatro (TO) ou área de operações (A Op) e que provê a proteção contra ações de exploração e ataque do oponente. A proteção é uma atividade de caráter permanente.

Por outro lado, exploração e ataque cibernéticos possuem conceitos distintos em diferentes referências. É de suma importância que os planejadores e executantes conheçam os limites de cada atividade para que haja um correto exercício do comando e para que limites estabelecidos não sejam transpostos.

Por estar em um domínio essencialmente artificial, a doutrina da defesa e da guerra cibernética obedecem a uma dinâmica de evolução mais veloz. Enquanto a ordem natural possui leis consideradas imutáveis do ponto de vista humano, o espaço cibernético está em permanente transformação, exigindo que os guerreiros que atuam nesse ambiente estejam em constante atualização. É plenamente compreensível que táticas, técnicas e procedimentos (TTP) cibernéticos devam se atualizar em uma frequência mais rápida que a de TTP aplicáveis aos outros domínios e que conceitos estabelecidos possam e devam ser revisados continuadamente.

ATAQUE CIBERNÉTICO

O ataque cibernético é uma capacidade operativa [2] que guarda estreita relação com a Função de Combate Fogos. Sua definição é dada pela doutrina de operações conjuntas: "conduzir ações sobre dispositivos, redes de computadores e comunicações do oponente para causar efeitos cinéticos e não-cinéticos". De acordo com o manual, o ataque cibernético busca atingir os seguintes objetivos ou efeitos:

> 1) destruir ou degradar equipamentos e sistemas, provocando baixas e/ou danos permanentes ou temporários, que sejam favoráveis à operação do TO/A Op;
> 2) degradar a capacidade de operação do oponente no campo de batalha, reduzindo a eficácia de funcionamento dos seus sistemas;
> 3) corromper dados de sistemas do oponente, manipulando informações de interesse do TO/A Op;
> 4) negar o acesso do oponente a sistemas de interesse do TO; e
> 5) interromper o funcionamento de sistemas do oponente que tragam vantagem ao TO.

Em virtude das características da guerra cibernética, para que o ataque cibernético seja realizado, faz-se necessária a exploração do ambiente cibernético de maneira a se obter o comando e controle de um sistema inimigo. Essa situação demanda o investimento de tempo, recursos financeiros e a aplicação de uma expertise sobre o espaço cibernético.

Normalmente, algumas etapas são seguidas para que seja possível julgar que determinada tropa cibernética é capaz de realizar um ataque, a saber:

1) **Reconhecimento:** o alvo é analisado de maneira a se encontrar uma ou mais vulnerabilidades que possam ser exploradas. Nessa etapa, os dados e informações encontradas em fontes abertas (*Open Source Inteligence* – OSINT, na sigla em inglês) são fundamentais. Um trabalho de engenharia social deve ser executado para levantar costumes e características do alvo ou de indivíduos ligados a ele ou, ainda, forçá-lo a proporcionar informações, tudo com o fim de se levantar uma vulnerabilidade passível de ser explorada. Essa etapa demanda um longo tempo e não deve ser desprezada. Quanto melhor for o reconhecimento executado, maiores serão as chances de êxito de um ataque cibernético.

2) **Armamento:** uma arma cibernética é desenvolvida para explorar a vulnerabilidade encontrada, objetivando provocar um determinado efeito. Um *exploit* específico é utilizado carregando consigo um *payload* para executar o efeito desejado. O *malware* desenvolvido precisa ser específico e suficientemente eficaz para escapar das defesas existentes no ambiente lógico a ser atacado.

3) **Entrega:** o artefato é disponibilizado ao alvo. Entendendo o alvo como um sistema [3], busca-se fazer com que o alvo tenha acesso ao *malware* desenvolvido. Diversas estratégias são empregadas para que a rede ou o ativo visado seja colocado em contato com o artefato desenvolvido. Muitas vezes, o ser humano é o vetor a ser explorado a fim de se acessar uma rede. Uma campanha de *phishing* ou mesmo *spear-phising* pode ser empregada para que determinado ator, previamente identificado, receba um e-mail com conteúdo malicioso. Em algumas vezes, uma vulnerabilidade até então desconhecida (e para qual ainda não há correção) é identificada e a entrega é realizada sem a necessidade da interação com um alvo humano.

4) **Exploração:** a ativação do *payload* é realizada e o *malware* é instalado no objetivo. Normalmente, essa etapa é dependente da participação do usuário, que habilita involuntariamente o código malicioso.

5) **Instalação:** O *malware* se consolida no alvo. Uma conexão com o exterior da rede visada é garantida por uma *backdoor* e a persistência dentro do alvo é estabelecida.

6) **Comando e Controle:** o atacante se estabiliza completamente dentro do alvo aproveitando o canal de comunicação estabelecido. A capacidade de realizar movimentos laterais na rede é explorada e a possibilidade de se fazer busca e exfiltração de dados e informações se torna uma realidade.

7) **Ações Objetivas:** uma vez que o comando e controle é estabelecido, o atacante pode executar ações para conseguir os efeitos desejados. Os efeitos de destruir, degradar, corromper dados, negar o acesso ou impedir o funcionamento podem ser plenamente alcançados.

O modelo apresentado toma por base o conceito da *cyber kill chain* e foi elaborado pela empresa fabricante de produtos de defesa *Lockheed Martin* para identificar e prevenir a atividades cibernéticas intrusivas. Esse *framework* ilustra muito bem os passos que um atacante precisa executar até conseguir provocar um efeito sobre um alvo. O ataque é somente a ação final de "detonar uma bomba", que foi customizada para penetrar nas defesas de um determinado alvo particular. A capacidade operativa de ataque cibernético só pode ser considerada factível por um

Fig 1 - Cyber Kill Chain® Lockheed Martin. Fonte: https://danieldonda.com/cyber-kill-chain/

decisor, se o comando e controle já tiver sido providenciado. Toda a ação anterior que prepara o terreno para a detonação da bomba, pela doutrina mais atual, não faz parte do ataque, mas sim da exploração cibernética.

> **“Assim como uma Bateria de Busca de Alvos dotada de radares e sistemas remotamente pilotados está intrinsecamente ligada à função de combate fogos, mas age como um vetor importantíssimo na função de combate inteligência, a tropa que realiza a exploração cibernética também atua nas duas funções de combate.”**

EXPLORAÇÃO CIBERNÉTICA

Segundo o MD30-M-01 – Doutrina de Operações Conjuntas (2020), toda a cadeia anterior às ações objetivas (ataque cibernético) está inserida no conceito da Exploração Cibernética, a saber: “mapear sistemas e ativos de informação presentes no Espaço Cibernético de interesse do TO/A Op [4], identificar vulnerabilidades e realizar a preparação para futuras ações ofensivas.”

Faz-se necessário desconflitar esse conceito com o previsto no manual do Exército EB70-MC-10.232 – Guerra Cibernética (2017). Enquanto o manual do Exército Brasileiro (EB), mais antigo, identifica a exploração cibernética como uma capacidade de “conduzir ações de busca ou coleta nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados”, igualando a exploração à inteligência cibernética; o manual do Ministério da Defesa (MD), mais atual, conceitua a exploração como uma etapa a ser realizada para a execução de um ataque.

Vale salientar que o manual EB70-MC-10.244 – Corpo de Exército (2020) já define a exploração cibernética em consonância com o manual do MD, ampliando o escopo da atividade e afastando-se do que postula o manual Guerra Cibernética.

A definição do MD está alinhada com o que prevê a doutrina conjunta dos Estados Unidos da América. O JP 3-12 – Cyberspace Operations, descreve uma gama de atividades incluídas nas ações de exploração do ciberespaço (*cyberspace exploitation)*. Para aquela nação, a exploração engloba tanto as atividades afetas a inteligência quanto as atividades preparatórias para a obtenção de um efeito (afetas ao ataque cibernético).

> A exploração cibernética inclui operações correntes e futuras por meio de ações como obter e manter acesso a redes, sistemas e nós com valor militar, manobrar para posições vantajosas e posicionar capacidades cibernéticas para facilitar operações futuras. [tradução nossa]

A Junta Interamericana de Defesa (JID) descreve o funcionamento de um ataque cibernético utilizando o modelo da *cyber kill chain*, ilustrando as diversas etapas que devem acontecer para que a obtenção de um efeito seja conseguida.

De acordo com a doutrina interamericana, o ataque cibernético se caracteriza pelo uso deliberado de uma arma cibernética para gerar um efeito prejudicial nas redes e sistemas de informação de um adversário, podendo ter efeitos indiretos no âmbito de operações convencionais.

Quando se refere aos tipos de operações, a JID define que a exploração cibernética se refere a procedimentos passivos ou ativos orientados a obtenção da informação necessária para a planificação e condução de operações cibernéticas defensivas e ofensivas ou outras operações convencionais. Dado que as operações cibernéticas ofensivas são definidas como aquelas executadas nas redes de adversários ou terceiros com a finalidade de causar um efeito cibernético ou um efeito físico, elas são dependentes de uma exploração

prévia, que permita a obtenção desses efeitos.

Em resumo, as doutrinas mais atuais, tanto do Brasil como de outros países, vinculam a possibilidade de um ataque cibernético à necessidade de uma exploração prévia. Da mesma maneira que um avião precisa ser armado, que uma bateria precisa entrar em posição e possuir um sistema de busca de alvos e que um torpedo precisa ser acondicionado no navio para que esses atuadores cinéticos possam atingir seus alvos e obter os efeitos desejados, uma tropa cibernética precisa explorar o ambiente cibernético para possibilitar a obtenção de um efeito do ataque do atuador não cinético. Vale salientar que a exploração já possui um caráter ofensivo e que a tropa opera em um "terreno inimigo".

A exploração, no entanto, pode se limitar a um reconhecimento em fontes abertas, agindo de maneira passiva. Nesse caso, não cumprirá sua missão precípua de preparar o terreno para a realização de um ataque. Essa preparação terá que, invariavelmente, realizar ações intrusivas.

Assim como uma Bateria de Busca de Alvos dotada de radares e sistemas remotamente pilotados está intrinsecamente ligada à função de combate fogos, mas age como um vetor importantíssimo na função de combate inteligência, a tropa que realiza a exploração cibernética também atua nas duas funções de combate. Quando se obtém o comando e controle para se realizar um ataque, o sistema do alvo já é plenamente conhecido e a extração de dados e informações passa a ser inteiramente possível.

Convém ressaltar que, muitas vezes, o decisor terá que optar entre obter um efeito (cinético ou não cinético) sobre um alvo ou permanecer com o comando e controle [5] de um determinado sistema para extrair dados e informações. Tem-se um exemplo prático: após instalar um *back door* em um sistema de comando e controle, ou mesmo de comunicações inimigo, um invasor pode apagar todos os dados do sistema, obtendo o efeito de degradar a capacidade de operação do inimigo, ou permanecer oculto no ambiente invadido para coletar informações sobre as posições das tropas inimigas no terreno. Uma escolha é feita: a cibernética será um atuador não cinético na função de combate fogos ou um vetor de busca de informações na função de combate inteligência. Ambas as ações exigem do guerreiro cibernético a adoção dos mesmos TTP, percorrendo toda a *cyber kill chain,* o que muda é apenas a provocação ou não de um determinado efeito na fase das ações objetivas.

A experiência tem mostrado que o sucesso de uma exploração cibernética é função do tempo investido nessa exploração, da expertise dos profissionais designados para essa tarefa e do volume de recursos financeiros disponibilizados para que os TTP possam ser executadas corretamente. Dessas variáveis, o tempo tem sido o fator com maior coeficiente. Quanto maior for a antecedência na designação de alvos para a cibernética, maior será a probabilidade de sucesso na coleta de dados e levantamento de informações, principalmente quando a atuação se limita a ações não intrusivas.

A CIBERNÉTICA COMO ATUADOR NÃO CINÉTICO DE FOGOS

No contexto do planejamento de fogos conjunto, a tropa cibernética é enquadrada como mais um atuador/vetor de fogos capaz de provocar efeitos sobre alvos previamente determinados. A etapa decidir do processo Decidir, Disparar, Detectar e Avaliar (D3A) busca definir, de antemão, quais os efeitos são desejados sobre quais alvos e quais são as tropas vocacionadas para obter esses efeitos. Como já explicitado, a possibilidade de ataque cibernético é diretamente dependente da exploração cibernética, o que demanda o investimento de tempo e recursos. Essa exploração, muitas vezes, terá de ser realizada desde os tempos pré-crise, o que acarreta a adoção de medidas para mitigar os riscos de se atuar no que se tem chamado de combate em zona cinzenta [6].

A Subseção de Guerra Cibernética, presente na Seção de Operações do Estado Maior Conjunto, é responsável por se integrar com os outros elementos de coordenação de fogos presentes nessa célula do Estado Maior Conjunto, a fim de apresentar as reais possibilidades de ataque dos Destacamentos de Guerra Cibernética presentes na campanha ou operação. A Proposta de Lista de Alvos da FCj G Ciber é, portanto, muito dependente da exploração cibernética previamente realizada.

Na reunião de Coordenação de Fogos, os alvos serão priorizados e será decidido qual o vetor de ataque será empregado sobre cada alvo, gerando a Lista Preliminar Integrada Priorizada de Alvos (LPIPA). Aspectos, como custo, tempo, possibilidades de cada tropa e riscos envolvidos, serão considerados para determinar qual meio provocará o efeito desejado sobre os alvos.

Após aprovação do comandante operacional (Cmt Op), a LPIPA deixa de ser provisória, tornando-se a Lista Integrada e Priorizada de Alvos (LIPA), e pode ser decomposta em Listas Priorizadas de Alvos (LPA) para cada Força Componente existente no TO ou A Op. A FCj G Ciber também receberá uma LPA contendo os alvos que devem ser batidos pelo atuador não cinético, a fim de cooperar com a obtenção do estado final desejado (EFD) estabelecido pelo Cmt Op.

PRIORIZAÇÃO DE ALVOS

A definição sobre qual atuador deverá bater cada alvo representa, em termos de força, espaço e tempo, como o comandante operacional visualiza a obtenção dos efeitos desejados que conduzem o esforço conjunto ao atingimento do EFD. Aspectos, como economicidade, riscos envolvidos para a tropa e para o cumprimento da missão, probabilidade de sucesso da investida, efeitos colaterais, além de vários outros fatores, são considerados para a escolha de um atuador em detrimento de outro.

Um ataque cibernético é normalmente mais econômico e envolto em menos riscos para a tropa. Em contrapartida, efeitos colaterais podem também existir no domínio cibernético, caso um *malware* destinado a um ativo escape para a rede mundial de computadores, afetando

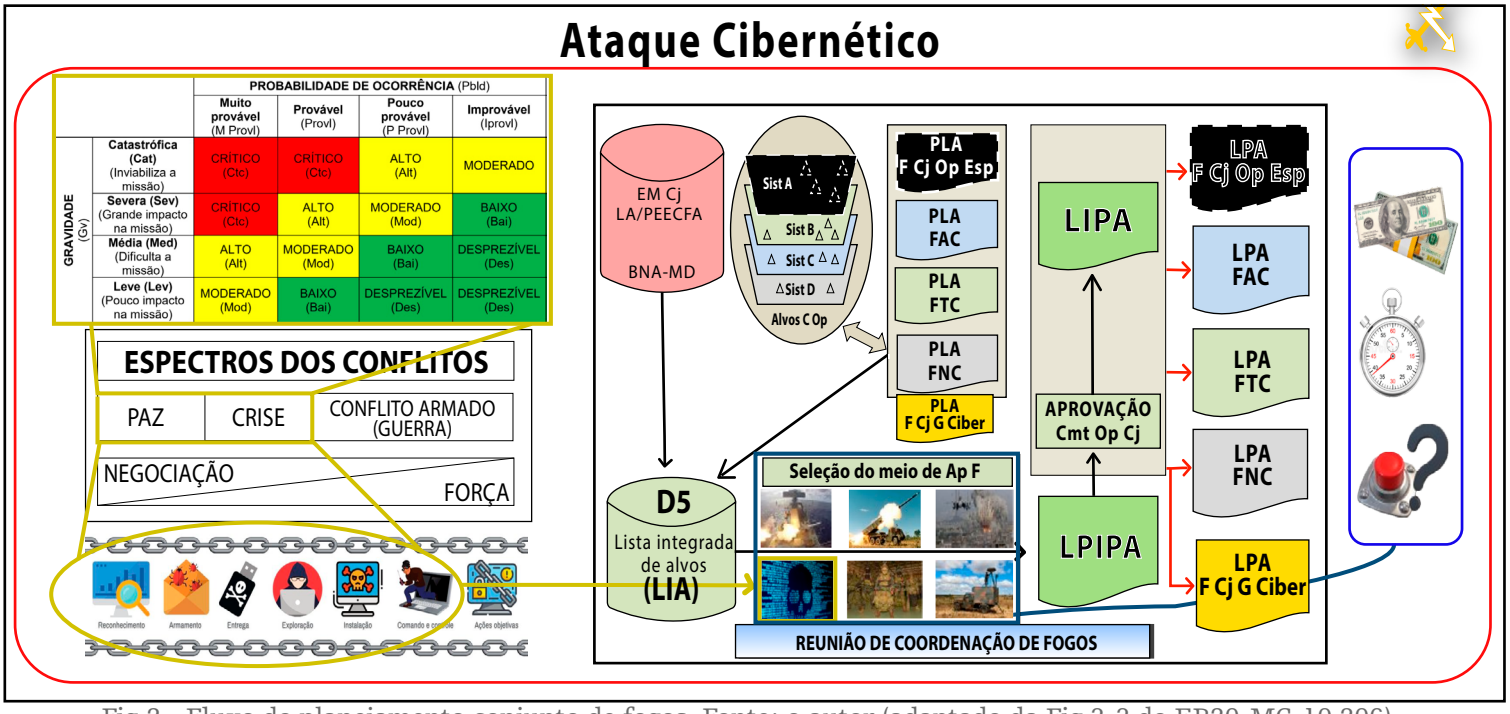

Fig 2 - Fluxo do planejamento conjunto de fogos. Fonte: o autor (adaptado da Fig 3-3 do EB20-MC-10.206).

Estados neutros, por exemplo. Em razão da artificialidade e da consequente mutabilidade do espaço cibernético, a probabilidade de sucesso de um ataque cibernético é um dado momentâneo e depende da exploração que foi realizada.

A Subseção de Guerra Cibernética é responsável por informar ao comandante qual a real capacidade da tropa cibernética para atingir os efeitos desejados. Enquanto os alcances da artilharia e o raio de ação dos aviões e navios são obtidos em função de dados reais, a capacidade da tropa cibernética só é conhecida após a realização da exploração. Daí a necessidade de se explorar o espaço cibernético desde os tempos pré-crise, tal qual faz-se necessário adquirir canhões e mísseis antes de a guerra começar.

CONSIDERAÇÕES FINAIS

A evolução tecnológica deixa um legado aos seres humanos ao ampliar a sua capacidade.

As limitações impostas pelo ambiente natural vão sendo vencidas e as Nações passam a contar com capacidades diversas para alcançar seus objetivos. O espaço cibernético foi desenvolvido como resposta da humanidade para lidar com o processamento de dados e com a automação de processos, gerando um ambiente que consolidou a globalização e possibilitou a alteração benéfica no modo de vida das pessoas.

Os interesses nacionais precisam ser mantidos também nesse novo domínio. A proteção dos ativos é uma necessidade constante e deve ser executada por cada ator que interage no ambiente cibernético.

As capacidades operativas de exploração e ataque representam a possibilidade de um país ampliar sua dissuasão para além do ambiente físico. Uma Nação não pode prescindir de seus canhões mesmo quando passa décadas sem travar guerras. Da mesma maneira, não se pode prescindir da capacidade de se obter efeitos no espaço cibernético e por meio dele.

REFERÊNCIAS

BRASIL. MINISTÉRIO DA DEFESA. GABINETE DO MINISTRO. **Portaria normativa Nr 3.010/MD, de 18 de novembro de 2020.** Aprova a Doutrina Militar de Defesa Cibernética (MD31-M-07).
BRASIL. MINISTÉRIO DA DEFESA. ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS**. Portaria normativa Nr 84/GM-MD, de 15 de setembro de 2020.** Aprova a Doutrina de Operações Conjuntas – MD30-M-01/Volumes 1 e 2 (2. ed. Brasília. 2020.
BRASIL. MINISTÉRIO DA DEFESA. EXÉRCITO BRASILEIRO. COMANDO DE OPERAÇÕES TERRESTRES. **Portaria Nr 42 – COTER, de 8 de junho de 2017.** Aprova o Manual de Campanha EB70-MC-10.232 Guerra Cibernética, 1ª ed. Brasília. 2017.
BRASIL. MINISTÉRIO DA DEFESA. EXÉRCITO BRASILEIRO. COMANDO DE OPERAÇÕES TERRESTRES. **Portaria Nr 66 – COTER, de 3 de junho de 2020.** Aprova o Manual de Campanha EB70-MC-10.244 Corpo de Exército, Edição Experimental. Brasília. 2020.
BRASIL. MINISTÉRIO DA DEFESA. EXÉRCITO BRASILEIRO. ESTADO MAIOR DO EXÉRCITO. **Portaria Nr 003-EME, de 5 de janeiro de 2015.** Aprova o Manual de Campanha EB20-MC-10.206. Fogos, 1 ed. Brasília. 2015.
EUA. SPECAL OPERATIONS COMMAND. **White Paper – The Gray Zone. 2015.** Disponível em: https://publicintelligence.net/ussocom-gray-zones/ Acesso em 11 set. 22.
EUA. Joint Chiefs of Staff. **Doctrine for the Armed Forces of the United States.** JP 3-12 Cyberspace Operations. Washington, DC: Joint Chiefs of Staff, 2018.
JUNTA INTERAMERICANA DE DEFENSA. **Guía de Ciberdefensa – Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar.** Canadá, 2020.

NOTAS

[1] O Exército Brasileiro também chama essas Capacidades Operativas de Atividades.
[2] Segundo o Glossário das Forças Armadas, capacidade operativa é o conjunto de capacidades específicas de unidades/elementos constituintes de uma Força, orientadas para a obtenção de um efeito estratégico, operacional ou tático.
[3] O alvo é percebido com um conjunto de elementos interconectados. Muitas vezes o objetivo final é uma peça que não possui um acesso disponível, mas possui ligação com outras partes cujo acesso é mais facilitado. O servidor de uma empresa é muito seguro, mas às vezes é colocado em rede com um laptop de um agente que utiliza a mesma máquina na rede de sua residência. A entrega não será feita ao servidor, mas ao agente, para que, por meio de futuros movimentos laterais (manobra), seja possível acessar o servidor.
[4] Teatro de Operações ou Área de Operações.
[5] Referindo-se à penúltima etapa da ciber kill chain. Etapa que antecede às ações objetivas.
[6] A zona cinzenta é definida pelo US Special Operation Command como interações competitivas entre e dentro de atores estatais e não estatais que se situam entre uma guerra tradicional e uma paz dual.

SOBRE O AUTOR

O Major de Artilharia Diogo Luiz Oliveira de Andrade é Oficial de Operações do Centro de Defesa Cibernética. Foi declarado Aspirante a Oficial pela Academia Militar das Agulhas Negras em 2005. Concluiu o Bacharelado em Ciências Econômicas pela Associação Educacional Dom Bosco em 2010, o Mestrado em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO) em 2013 e a Pós-Graduação em Ciências Militares pela Escola de Comando e Estado Maior do Exército (ECEME) em 2021. Realizou cursos na área segurança de rede de computadores e Artilharia de Mísseis e Foguetes. Cursou o Field Artillery Captains Career Course, em Fort Sill, EUA, o Curso de Armas Combinadas, na Escuela Superior Tecnológica del Ejército, Bolívia e realizou a capacitação em Ciberdefensa, da Junta Interamericana de Defesa (JID) (diogoluiz@cdciber.eb.mil.br).