MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE ALEXANDRINO

CURSO DE APERFEIÇOAMENTO AVANÇADO EM
SEGURANÇA DA INFORMAÇÃO E COMUNICACÕES

TRABALHO DE CONCLUSÃO DE CURSO

GUERRA CIBERNÉTICA E GUERRA TRADICIONAL: A COMPLEXA TEIA DOS CONFLITOS MODERNOS

PRIMEIRO-TENENTE MATEUS PORTO DE ALMEIDA

Rio de Janeiro
2023

PRIMEIRO-TENENTE MATEUS PORTO DE ALMEIDA

GUERRA CIBERNÉTICA E GUERRA TRADICIONAL: A COMPLEXA TEIA DOS CONFLITOS MODERNOS

Monografia apresentada ao Centro de Instrução Almirante Alexandrino como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança Da Informação e Comunicações.

Orientadores:
Capitão-Tenente WARLLEY PAULO FREIRE
Capitão-Tenente MARCOS JOSÉ BARBOSA FILHO

CIAA
Rio de Janeiro
2023

PRIMEIRO-TENENTE MATEUS PORTO DE ALMEIDA

GUERRA CIBERNÉTICA E GUERRA TRADICIONAL: A COMPLEXA TEIA DOS CONFLITOS MODERNOS

Monografia apresentada ao Centro de Instrução Almirante Alexandrino como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança Da Informação e Comunicações.

Aprovada em ____ de _____ de 2023

Banca Examinadora:

_____

CMG (RM1-EN) Gian Karlo Huback Macedo de Almeida – CIAW

_____

CT Warley Paulo Freire – CoNavOpEsp

_____

CT Marcos José Barbosa Filho – NAsH Dr. Montenegro

CIAA
Rio de Janeiro
2023

Dedico esse trabalho a Deus e a minha família que sempre estiveram comigo, me apoiando para o meu desenvolvimento moral e intelectual.

AGRADECIMENTOS

Ao término deste trabalho, sinto uma imensa gratidão pela minha derrota de aprendizado e dedicação durante esse ano realizando o C-Ap-A. Gostaria de expressar meus sinceros agradecimentos a todos que me auxiliaram para o meu crescimento acadêmico e profissional.

Primeiramente, gostaria de agradecer à Deus por ter estado comigo em todas as minhas dificuldades e ter me dado força para minhas realizações.

À Marinha do Brasil por me proporcionar a oportunidade de aprimorar meus conhecimentos por meio deste curso. É uma honra servir em uma instituição que valoriza a educação e o desenvolvimento de seus militares

Ao coordenador do curso, CMG(RM-1) Huback, por estar sempre pronto para auxiliar nas necessidades apresentadas, aos meus orientadores, CT Freire e CT Marcos Barbosa quero expressar minha profunda gratidão. Suas orientações, ensinamentos e paciência foram fundamentais para meu sucesso neste curso. Seus conhecimentos e experiências compartilhadas foram inestimáveis.

À minha família e a minha namorada Emília, expresso minha gratidão por seu constante apoio e incentivo. Seu amor e compreensão tornaram possível minha dedicação aos estudos e minha busca por excelência.

"De poder ao homem, e descobrirá quem ele realmente é."
Maquiavel

GUERRA CIBERNÉTICA E GUERRA TRADICIONAL: A COMPLEXA TEIA DOS CONFLITOS MODERNOS

Resumo

A interação entre a guerra cibernética e a guerra tradicional é um elemento complexo do cenário de conflito moderno. A dependência crescente da tecnologia e da conectividade acaba por desempenhar um dos papeis centrais nas estratégias militares atuais. Um exemplo notável dessa interação é o grupo *Turla*, que tem sido associado a ataques cibernéticos direcionados a instituições governamentais e militares. Esses ataques mostram como adversários podem explorar vulnerabilidades tecnológicas para obter informações estratégicas e comprometer a segurança nacional.

O *malware Stuxnet* representa um marco na história da guerra cibernética. Esse *worm*, altamente sofisticado, foi projetado para sabotar sistemas de controle industrial, incluindo aqueles usados em instalações nucleares. Isso demonstra como a guerra cibernética pode ser usada para atacar infraestrutura crítica, uma tática que pode ser diretamente relacionada a conflitos tradicionais, representando uma imensa ameaça.

Além disso, a guerra cibernética pode se estender a ataques a meios navais e sistemas de defesa, com o potencial de desestabilizar operações navais convencionais. Dessa forma a cibersegurança deve se tornar uma parte crucial da segurança militar, uma vez que a exposição de sistemas de defesa e de infraestrutura naval a ataques cibernéticos pode ter sérios efeitos.

Dessa forma, a interação entre guerra cibernética e guerra tradicional é uma realidade complexa e mutável. A dependência da tecnologia é evidente em conflitos modernos, e a compreensão desses desafios é fundamental para garantir a segurança e a estabilidade internacionais. Os exemplos de ataques do grupo *Turla*, o *Stuxnet* e ataques a meios navais destacam como a guerra cibernética pode influenciar diretamente o cenário de conflito tradicional, criando desafios significativos para a segurança e a defesa.

Palavras- chave: Guerra Cibernética; Guerra Tradicional; *Stuxnet*; *Malware* e Meios Navais.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTAS DE SIGLAS E ABREVIATURAS

END	Estratégia Nacional de Defesa
TI	Tecnologia da Informação
MB	Marinha do Brasil
APT	Ameaça Persistente Avançada
C2	Comando e Controle local
DLL	*Dynamic Link Library*
ICS	Sistema de Controle Industrial
PLC	Controladores Lógicos Programáveis
NCS	Sistemas Controlados por Rede
RTE	*Real-Time Ethernet*
BSA	*Backtrack Search Optimization Algorithm*
COP	*Timers Computer Operating Properly*
MitM4	*Men in the Middle*
IFW	Implementação de *firewall*
IADS	Sistema de detecção de intrusão e anomalia

SUMÁRIO

1. INTRODUÇÃO

Muita das vezes torna-se sugestivo pensar que a busca pelo desenvolvimento tecnológico do homem está atrelada a sua vontade de se sobrepor a natureza, tal como sugere a expressão muito disseminada " A conquista da natureza pelo homem", embora em alguns casos isso possa ser aplicável, em via de regra não é através desse modelo que a estrutura da realidade se projeta (Lewis, 1943).

A partir da ideia supracitada, o avião pode ser a base para um excelente exemplo, esse meio de transporte é um dos símbolos máximos da sobreposição da humanidade a natureza, a capacidade do homem de voar. De forma geral, qualquer pessoa em uma sociedade pacífica pode-se utilizar desse meio desde que pague, porém, falar que o usuário esta exercendo seu poder sobre a natureza seria um equívoco. A partir do momento que se necessita pagar para que alguém o leve a algum lugar, não se pode dizer que este indivíduo seja um homem que dispõe do real poder de se sobrepor a natureza, pois esta sujeito a vontade daqueles que vendem, ou por aqueles que permitem que sejam vendidas, ou por aqueles que possuem os meios de produzi-las, ou por aqueles que as produzem (Lewis, 1943).

> Aquilo que chamamos de poder do Homem é, na realidade, um poder que alguns homens possuem, e que por sua vez podem ou não delegar ao resto dos homens. Sob esse ponto de vista, o que chamamos de poder do Homem sobre a Natureza se revela como um poder exercido por alguns homens sobre outros, com a Natureza como instrumento (Lewis, 1943).

A partir desse conceito inicial é perceptível que o cenário geopolítico tem mudado com o passar dos anos, as ameaças do século XXI são distintas das que eram observadas nos séculos anteriores. Contudo, seus fins ainda se mantêm, a busca por espaço e poder. Dentro dessa lógica as formas de combate têm se adaptado e evoluído no decorrer da história como forma de melhor se sobrepor ao seu oponente.

Como exemplos temos os grandes avanços tecnológicos no decorrer dos conflitos do século XX, a 1ª Guerra Mundial (1914-1918) e 2ª Guerra Mundial (1939-1945). A máquina Enigma, que criptografava e descriptografava códigos, sendo considerada ponto chave na invasão dos meios de comunicação estratégicos. (Krischer, 2013). O químico alemão Fritz Harber (1868-1934), que ganhou o Nobel de química em 1918, foi um dos principais desenvolvedores dos gases tóxicos usados na Primeira Guerra. Tendo Harber como aliado científico, o exército alemão proporcionou à história

das guerras uma das mais terríveis cenas de mortes em massa, na cidade de Yprès, na Bélgica. (Fernandes, 2013).

O desenvolvimento tecnológico seguiu no decorrer da Guerra Fria (1947-1989), período em que o mundo se polarizou e as principais potências do mundo (União Soviética e Estados Unidos) utilizavam-se das suas descobertas científicas como forma de projetar seu poder e superioridade sobre o mundo, além de intimidar uma a outra (Reynol, 2002). Nesse contexto da primeira rede de computadores entrou em funcionamento em 1969 (Castells, 2005). Com objetivo de auxiliar a troca de informações em um sistema de compartilhamento de informações entre pessoas geograficamente afastadas, buscando facilitar as estratégias de guerra.

Destaca-se também a corrida espacial muito fomentada durante esse período, na busca incessante em se mandar o homem a lua, que possibilitou o aperfeiçoamento de lançamento de diversas tecnologias nas áreas de lançamentos de foguetes entre outras (Reynol, 2002).

Após a Guerra Fria, o ciberespaço passou a ser utilizado como estratégia militar, principalmente em função dos avanços tecnológicos e das novas descobertas. A guerra cibernética acontece no ciberespaço e não pode ser mensurado. À proporção que a área é desenvolvida aumentam também os riscos atrelados a ela. A Marinha do Brasil possui algumas singularidades visto que é uma instituição militar e tem seus critérios distintos do meio civil. Além disso, com novos cenários e ameaças, novas interpretações também variam de acordo com a conjuntura. A internet por si só alterou essas percepções.

No que tange a Guerra Cibernética, o Governo Federal, o Ministério da Defesa e a Marinha do Brasil estão buscando ferramentas para encarar a nova realidade. Em 2008 foi publicada a Estratégia Nacional de Defesa (END) na qual o setor cibernético teve sua gerência destinada ao Exército Nacional. Nacionalmente, o Grupo Técnico de Segurança Cibernética foi criado em 2009. O setor cibernético é considerado estratégico para a defesa nacional, assim como os setores nuclear e espacial (BRASIL, 2012). Nota-se a crescente importância da Tecnologia da Informação (TI) no cenário mundial, inclusive na Marinha do Brasil (MB).

Assim, esse trabalho visa auxiliar na melhoria da defesa cibernética da MB fornecendo informações, *insights* e orientações atualizadas. Ao analisar ameaças cibernéticas recentes, tendências e melhores práticas. Além de orientar os militares desta instituição, buscando o aumento da mentalidade de segurança cibernética, dessa

forma, ajudando a prevenir ataques, detectar atividades maliciosas e responder de maneira eficaz a incidentes virtuais.

1.1 Apresentação do Problema

Apesar da não ocorrência de um conflito cibernético global, diferente dos conflitos cinéticos. As informações coletadas das guerras cibernéticas devem ser armazenadas, mesmo que suas ocorrências se limitem as poucas décadas passadas, e que sua quantidade seja muito mais ínfima, se comparado as informações derivadas de conflitos cinéticos que se acumulam através de milênios. Analisar os poucos embates no campus virtual são uma excelente forma de prever problemas futuros (Sá, Machado e Almeida, 2019).

Mergulhado na conjuntura de constantes avanços tecnológicos, bem como a sua utilização para ofensivas entre países, como nos casos do *Stuxnet* que realizou um ataque a estrutura da usina nuclear iraniana ou do grupo *Turla* que realizou ações de espionagem em diversos países. Torna-se evidente a possibilidade de existências de diversas vulnerabilidades em que a MB pode estar sujeita. Havendo assim, a necessidade de à cada dia correlacionar a estrutura da guerra cibernética com as doutrinas mais tradicionais encontradas no combate clássico com propósito de reduzir esses riscos.

Dessa forma, este trabalho visa expor aos integrantes da MB, as diversas formas de ataques presentes no ciberespaço e como esses podem afetar diretamente a estrutura essências de uma nação, assim como trazer risco ao Poder Naval. Uma vez que a mentalidade da Segurança Cibernética ainda não é algo tão inerente ao setor marítimo. Dado exemplo de que, muitos destes possuem a percepção errônea de que os sistemas que operam a bordo encontram-se seguros de ofensivas virtuais, através do isolamento físico e lógico de seus sistemas críticos, estratégia conhecida como *air-gap*[1].

[1] Isolamento físico ou lógico usado para proteger sistemas de computadores ou redes de acesso não autorizado, especialmente contra ataques cibernéticos.

1.2 Justificativa e Relevância

Ante ao contexto de desenvolvimento tecnológico atual, a integração surge como uma marca e um fator que possibilita um notório aumento da produtividade dos setores, no entanto, apresentando um paradoxo com o crescimento da vulnerabilidade dos mesmos. Os ataques cibernéticos têm sido utilizados para afetar diversos setores da sociedade desde empresas de grande, médio e pequeno porte até contra governos inteiros como no caso do ataque a Usina Nuclear de Natanz no Irã e do grupo *Turla*. Os setores militares também ficam expostos a essas evoluções, inclusive no que tange a área naval. Sendo assim, esse trabalho tem o propósito de trazer a consciência a necessidade de adaptação dos meios navais aos diversos tipos de perigos cibernéticos que o mundo moderno pode oferecer.

1.3 Objetivos

1.3.1 Objetivo Geral

Essa pesquisa tem como objetivo geral analisar a utilização de *malwares* em um contexto de guerra cibernética e como o emprego dessas técnicas ao longo do tempo vem se tornando uma das principais metodologias de ataque. Ressaltando suas principais caraterísticas de ações assimétricas e ocultação de autoria. Mostrando como tais aplicações podem afetar também a Estrutura Naval.

1.3.2 Objetivos específicos

Além disso, a pesquisa tem como finalidades específicas:

- Apresentar como a evolução da tecnologia tem afetado diretamente os conceitos da Guerra Tradicional; assim como conscientizar a respeito das novas tecnologias que fazem parte dos domínios do conflito e da segurança internacional atual;
- Demostrar o funcionamento dos ataques cibernéticos relacionados ao *Stuxnet* e ao grupo *Turla* e seus respectivos impactos e consequências em âmbitos domésticos e internacionais, da política e da segurança, tanto física

quanto virtual;

- Demostrar as principais técnicas de ataques ligadas a Indústria Naval e como os ataques as cadeias de suprimentos podem ser o modo mais efetivo para uma possível contaminação; e
- Debater técnicas para o aumento do nível de defesa, assim como formas para elevar a consciência sobre a segurança para os principais atores ligados aos meios navais.

1.4 Contribuições

O estudo dos ataques cibernéticos e da segurança cibernética desempenham um papel crucial na proteção de um país e pode trazer várias contribuições importantes como auxiliar na identificação de vulnerabilidades em infraestruturas críticas, permitindo que as autoridades tomem medidas proativas para corrigi-las antes que sejam exploradas por adversários.

Além disso, compreender como os ataques cibernéticos são conduzidos auxilia para que os especialistas em segurança cibernética desenvolvam estratégias de prevenção mais eficazes. Isso inclui a criação de políticas, regulamentações e práticas recomendadas para proteger ativos críticos. Sendo assim, de posse de um conhecimento mais refinado, a capacidade de resposta a incidentes tende a aumentar. Isso envolve a criação de planos de resposta a incidentes, treinamento de pessoal e a coordenação eficaz entre agências de segurança.

O desenvolvimento da estrutura de defesa é um intento que pode ser alcançado com a pesquisa de ataques cibernéticos como a evolução de *firewalls*, sistemas de detecção de intrusões e ferramentas de análise de ameaça. Tal qual, um aumento da consciência sobre os riscos cibernéticos em todos os níveis da sociedade, vem levando a uma maior adoção de práticas seguras de computação em todos os setores.

Com isso, a proteção contra ataques de Ameaça Persistente Avançada (APT[2]) direcionados a dados governamentais e financeiros que representam uma ameaça séria à segurança e estabilidade tendem a se tornar mais eficazes. Ressalta-se que esses

2 Termo usado em cibersegurança para descrever ataques cibernéticos altamente direcionados e persistentes. Essas ameaças são conduzidas por atacantes sofisticados, como governos ou grupos cibercriminosos, que têm recursos significativos e objetivos específicos.

atacantes são altamente sofisticados, costumando ser compostos por grupos cibercriminosos ou até mesmo nações, visando sempre obter acesso não autorizado a informações confidenciais, dados financeiros sensíveis e segredos de Estado. Esses ataques não apenas comprometem a integridade e a privacidade dos dados, mas também podem resultar em consequências graves, incluindo espionagem, fraude financeira e sabotagem.

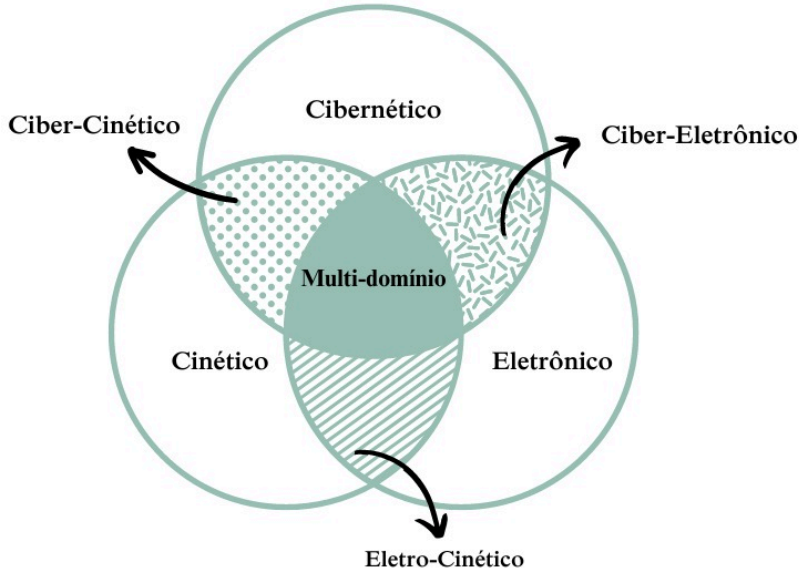
2. REFERENCIAL TEÓRICO

2.1 Contexto Político

Inicialmente, antes de aprofundar de forma detalhada nos conceitos de técnicas de ataque cibernéticos, considera-se de grande valia, ampliar a visão do leitor sobre como esses métodos estão inseridos dentro dos conceitos de cada campo dos domínios das táticas de guerra.

De forma a melhor elucidar tal perspectiva, Sá, Machado e Almeida (2019) explicam o fenômeno da interação entre as áreas cibernética, eletrônica e cinética em operações de guerra em gráfico que demonstra mútuas influências entre as áreas.

Figura 1 - Domínios da guerra.



Fonte - Sá, Machado e Almeida (2019*)*.

Segundo Sá, Machado e Almeida (2019) a classificação ciber-cinética como ações que objetivam causar efeitos no mundo físico através de ataques à sistemas computacionais. O campo ciber-eletrônico é aquele onde ações de guerra eletrônica buscam atingir sistemas computacionais, corresponderia a uma nova etapa evolutiva de ataques eletrônicos. Nesse caso, o espectro eletromagnético é utilizado pelo atacante para enviar um fluxo de dados ao processador do sistema alvo de forma a manipular seu processo computacional, comprometendo assim o seu funcionamento. Já o campo eletro-cinético estabelece uma relação entre o mundo físico e o espectro eletromagnético, de acordo com os autores, um exemplo de aplicação seria a utilização de minas magnéticas. Nessas minas, a detonação, efeito físico, é realizada através da detecção do campo eletromagnético gerado por estruturas metálicas.

O presente trabalho busca desenvolver algumas técnicas de ataques atinentes aos subconjuntos relacionados aos conceitos de Cibernético e Ciber-Cinético. De forma geral, os ataques cibernéticos podem ser usados como ferramentas de espionagem, sabotagem e desestabilização. Além disso, muitas vezes são considerados extensões dos conflitos do mundo real, devido à sua capacidade de causar impacto significativo em governos, organizações e indivíduos.

Segundo Hjortdal (2011), o ciberespaço é essencial na guerra moderna em diversos níveis. Seja ele operacional, onde os soldados estão cada vez mais dependentes do ciberespaço, assim como em níveis estratégicos, onde os pontos fortes e fracos de um Estado no ciberespaço podem ser usados para dissuadir e afetar o equilíbrio estratégico de poder.

O IISS (2010) considera a guerra cibernética como um campo intelectualmente subdesenvolvido. Contudo, afirma que o futuro conflito entre Estados pode ser caracterizado pelo uso das chamadas técnicas assimétricas. A principal delas pode ser o uso da guerra cibernética.

No que tange a dinâmica do domínio do ciberespaço, nota-se que normalmente é mais fácil atacar do que defender. De acordo com a Revisão Quadrienal de Defesa dos EUA de 2010, “a velocidade dos ataques cibernéticos e o anonimato do ciberespaço favorecem enormemente o crime, pois financeiramente torna-se mais barato, além de demandar uma capacidade técnica inferior."

A partir desse princípio lógico, Hjortdal (2011) faz a seguinte declaração em seu artigo:

> Também se pode esperar que o Ocidente e os Estados Unidos, por exemplo, ajam de forma semelhante ao que a China é acusada de fazer. No entanto, uma análise das capacidades americanas não é o tema aqui, uma vez que os Estados Unidos não têm tanto a ganhar relativamente contra a China, desenvolvendo uma capacidade cibernética agressiva. Isto pode ser visto à luz das três razões anteriormente citadas pelas quais os estados procuram manter e utilizar tal capacidade. Em primeiro lugar, os Estados Unidos não precisam de dissuadir outros Estados através do ciberespaço, uma vez que administram muito bem militarmente. Em segundo lugar, a realidade atual é que, uma vez que a tecnologia militar dos EUA é incomparável, a espionagem intensiva para obter conhecimento vantagem sobre a tecnologia militar de outros estados não é necessária. Quanto à terceira razão relativa à vantagem económica, a espionagem industrial tem menos significado para os Estados Unidos, uma vez que os níveis tecnológicos industriais nos Estados Unidos estão entre os mais avançados do mundo.

Dessa forma, torna-se notório que os ciberataques servem como uma grande arma para os países menos favorecidos, tanto em poderio militar quanto econômico sobre os países mais abastecidos. De modo, que tal sistemática de ataque acaba por performar como uma " guerrilha moderna".

Utilizando o gráfico apresentado na Figura 1 de Sá, Machado e Almeida (2019), a guerrilha estaria inserida no âmbito cinético e eletro-cinético, o que seriam parâmetros muito afastados da sistemática proposta neste trabalho, no entanto seus princípios lógicos aplicados são muito semelhantes aos ciberataques.

Os ciberataques compartilham algumas semelhanças conceituais com a guerrilha em termos de conflito assimétrico e uso de táticas defensivas e ofensivas. No entanto, eles são distintos em termos de meio, natureza da destruição e estratégias envolvidas. Os ciberataques representam uma forma moderna de conflito que ocorre no espaço digital, enquanto a guerrilha é uma forma de conflito físico e territorial.

Nos dias atuais a China vem se firmando cada vez mais como uma potência no campus das ofensivas cibernéticas, demostrando a importância das adoções de tais estratégias de combate. Como exemplo Hjortdal (2011) destaca que no Reino Unido, um documento de 14 páginas do MI5[3] chamado "A Ameaça da Espionagem Chinesa", elaborado em 2008, chegou agora às esferas públicas. O relatório anteriormente restrito

[3] Agência de inteligência doméstica do Reino Unido.

dizia que “qualquer empresa do Reino Unido pode estar em risco se possuir informações que beneficiem os chineses”

Ao utilizar tais medidas surge a possibilidade de equiparação de poder com a maior potência bélica do mundo atual, o EUA. Dessa forma a utilização de tais técnicas assimétricas no jogo de poder, acabam por difundir a cada dia mais (Hjortdal, 2011).

Além de todos os prejuízos estruturais e financeiros causados pelas investidas virtuais, o mesmo ainda é causador de diversos desgastes políticos devido a facilidade em se ocultar a autoria da ofensiva (Hjortdal, 2011).

Mesmo que a maioria dos ataques que serão descritos neste trabalho, não relatem atos praticados contra belonaves, embarcações civis ou infraestruturas existentes nas margens, sob ou sobre a superfície da água. As informações coletadas servirão como referência para a construção de possíveis situações que deixariam os meios navais em situações vulneráveis. Além de trazer à tona relevância do estudo dos conflitos cibernéticos para o contexto da guerra tradicional.

A partir dos conceitos anteriormente citados, percebe-se a grande importância para o Estado em desenvolver uma maior capacidade cibernética, dentre as quais destacam-se:

- Adquirir maior conhecimento através da espionagem no ciberespaço; e
- Dissuadir outros Estados infiltrando-se nas suas infraestruturas críticas.

2.2 Estado da Arte

No que se refere aos ataques através de espionagem no ciberespaço, pode se destacar um grupo conhecido por seus diversos ataques realizados, conhecido como *Turla*. O grupo é considerado um APT, conhecido por suas atividades de ciberespionagem direcionadas a governos e organizações estratégicas em todo o mundo. Eles são conhecidos por suas habilidades técnicas superiores e por suas operações de longo prazo.

No tocante as ofensivas contra infraestruturas críticas, tem-se como referência o Stuxnet, um malware altamente complexo e notório que teve como alvo sistemas de controle industrial, causando danos físicos da Usina Nuclear de Nataz no Irã (Espinosa, 2021). Ele é amplamente considerado como um exemplo pioneiro do artefato cibernético que trouxe à tona questões significativas sobre cibersegurança, guerra cibernética e atribuição de ataques cibernéticos.

2.3 *Turla* - Ofensivas por espionagem

2.3.1 Estrutura e objetivos

Segundo Faou (2019), o Turla, também é conhecido como *Snake*, um dos grupos de ciberespionagem mais antigos e ainda ativo, com mais de uma década de experiência. Os seus operadores concentram-se principalmente em alvos de alto perfil, como governos e entidades diplomáticas na Europa, Ásia Central e Médio Oriente. O grupo é conhecido por ter violado grandes organizações como o Departamento de Defesa dos EUA, em 2008, e a empresa de defesa suíça RUAG, em 2014. Mais recentemente, vários países europeus, incluindo a França e a República Checa, denunciaram publicamente os ataques de Turla contra os seus governos.

De acordo com Faou (2019), após anos de pesquisa sobre as localidades e tipos de vítimas que foram atingidas por esse grupo, concluiu-se que o *Turla* visa organizações que possam trazer maior risco a estrutura de uma nação, como:

- Ministérios das Relações Exteriores e representações diplomáticas (embaixadas, consulados, etc.);
- Organizações militares;
- Organizações políticas regionais; e
- Empreiteiros de defesa.

Outro fato notório é a inexistência de relatos de ataques desse grupo, sendo executado na Ásia Oriental. Dentre as vitimas de alto-perfil pode-se destacar:

Figura 2 - Linha do tempo de ataques importantes atribuídos ao grupo Turla

Fonte: Faou (2019).

2.3.2 Funcionamento

Tal grupo utiliza-se de diversas técnicas e *malwares* para auxiliar a alcançar seus objetivos, essas técnicas de propagação tendem a ser simples. Algumas vezes os

métodos precisam ser adaptados de acordo com o alvo. Para isso, o *Turla* possui um amplo arsenal para ser utilizado nas principais plataformas de *desktop* sejam elas *Windows, macOS* e *Linux* (Faou, 2019). Dentre esses artifícios destacam-se:

- E-mails de *phishing*[4] com *exploits*[5] do Adobe PDF;
- Engenharia social para induzir o usuário a executar instaladores de malware com extensão ".SCR[6]", muitas vezes compactados com RAR;
- Ataques de *watering hole*[7] que usam *exploits* do Java (CVE-2012-1723), do Adobe *Flash* (desconhecidos) ou do Internet Explorer 6, 7, 8 (desconhecidos); e
- Ataques de *watering hole* que contam com a engenharia social para induzir o usuário a executar falsos instaladores do "*Flash Player*".

No entanto, as técnicas anteriormente relatadas, somente descrevem os métodos de compartilhamento, não detalhando o comportamento e as ferramentas utilizadas pelo atacante após adentrar um sistema. Sendo assim, no que concerne a esse tipo de informações, destacam-se:

> Dos muitos recursos fornecidos pela plataforma de espionagem *Turla*, o registro de pressionamentos de teclas e dados ambientais é o foco central. Como parte de sua carga útil, *Turla* aproveita *SetWindowsHookEx* para coletar e registrar as teclas digitadas junto com outros dados do sistema. O manipulador de gancho do *Turla* executa um número substancial de operações por pressionamento de tecla e para descobrir manualmente as ações tomadas são necessários dias de engenharia reversa de nível especializado (Case et. al., 2020).

Visando um melhor entendimento do leitor, ressalta-se que o conceito de *SetWindowsHookEx* baseia-se em uma função da API(Interface de Programação de Aplicativos) do *Windows* que é usada para criar um *hook* (gancho) do sistema ou de aplicativo em um sistema *Windows*. Enquanto os *hooks* são mecanismos usados para

---

[4] Técnica de engenharia social usada por cibercriminosos para enganar e induzir pessoas a revelarem informações confidenciais.

[5] Programa ou código de software que aproveita uma vulnerabilidade em um sistema.

6 Extensão de arquivo geralmente é associada a arquivos de código-fonte.

[7] Tipo de ataque cibernético direcionado que visa infectar os visitantes de um site específico.

monitorar eventos do sistema ou do aplicativo em um nível mais baixo do que uma aplicação normalmente teria acesso. Isso permite que um programa "gancheie" ou intercepte eventos específicos e tome medidas com base nesses eventos (Case et. al., 2020).

Embora o *Turla* utilize *malwares* sofisticado como o *rootkit* [8], este trabalho fundamentara as movimentações do grupo relacionadas ao *malware* conhecido como *LigthNeuron*. Esse software malicioso pode ser considerado relativamente simples, se comparado aos demais utilizados pelo grupo. No entanto, o *LigthNeuron* se destaca pela sua grande capacidade de furtividade (Faou, 2019).

Segundo National Cyber Security Centre (2017), o *Neuron* é usado para infectar infraestrutura de rede, como servidores de correio e web, e atua como Comando e Controle local (C2). O estabelecimento de um C2 local limita a interação com a rede de destino e hosts remotos. A instalação de um servidor C2 dentro da rede da vítima permite que o ator evite a detecção pelo monitoramento baseado em gateway de rede. Embora as comunicações externas sejam necessárias para que o ator estabeleça conexões de volta à sua infraestrutura C2 *upstream*, essas comunicações são frequentemente criptografadas usando a configuração TLS legítima da rede da vítima.

De acordo com o National Cyber Security Centre (2017), um dos métodos de comunicação entre o cliente e o serviço *Neuron* é por meio de solicitações HTTP. O serviço *Neuron* cria seu próprio *listener* HTTP e aguarda solicitações para um endpoint de URL do *Neuron* configurado. Esses nomes de endpoint têm como tema serviços da Web legítimos, como *Microsoft Exchange* e *Microsoft IIS*, o que ajuda ainda mais o tráfego de malware a parecer legítimo. Os detalhes desses endpoints são fornecidos na seção Comunicações de serviço do Neuron deste comunicado (National Cyber Security Centre, 2017).

De acordo com Faou (2019):

> O LightNeuron é um malware projetado para atingir servidores Microsoft Exchange. Ele tem duas facetas: espionar emails e atuar como um backdoor completo. Até onde se sabe, aproveitar um agente de transporte do Microsoft Exchange para persistência é algo único e nunca antes visto. Além disso, nos poucos casos que estudamos, o Light Neuron estava rodando com privilégios SYSTEM. Normalmente é difícil obter esse nível de privilégio em um

8 Malware projetado para se esconder profundamente no sistema operacional de um computador ou dispositivo, frequentemente com privilégios de administrador.

> servidor Microsoft Exchange, pois é um dos ativos mais críticos de uma organização. Assim, uma vez comprometido, é provável que permaneça sem ser detectado durante meses ou anos.

Segundo National Cyber Security Centre (2017), o vetor de infecção do *Neuron* normalmente ocorre por meio do abuso de vulnerabilidades da camada de aplicativo no *software* do servidor, configurações incorretas do servidor ou ataques de força bruta em contas administrativas. O *Neuron* requer um serviço que essencialmente executa as mesmas ações que o serviço do cliente, incorporando a carga final usando o mesmo método detalhado na seção Cliente *Neuron*.

Como forma de modelar tal conceito, tem-se o exemplo da atuação do *Ligth Neuron* no *Microsoft Exchange*, onde os dois principais componentes do *malware* atuam, sendo eles (Faou, 2019):

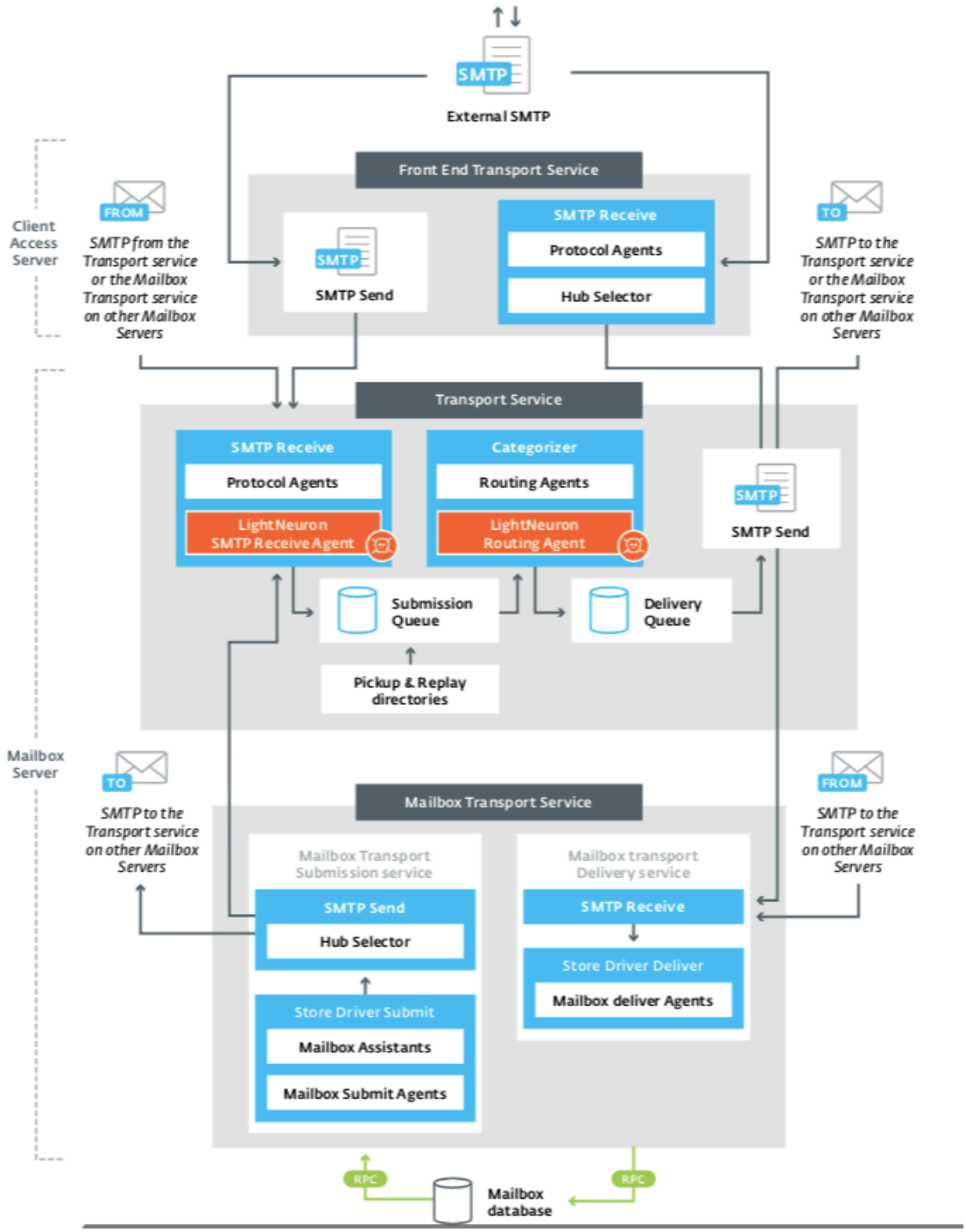
- Agente de Transporte, registrado na configuração do *Microsoft Exchange*; e
- *Dynamic Link Library* (DLL) complementar de 64 bits contendo a maior parte do código malicioso.

O Agente de Transporte tem uma função importante no *Microsoft Exchange* como bem explica Faou (2019):

> O *Microsoft Exchange* permite estender suas funcionalidades utilizando Agentes de Transporte que podem processar e modificar todas as mensagens de email que passam pelo servidor de email. Os Agentes de Transporte podem ser criados pela *Microsoft*, por fornecedores terceirizados ou diretamente dentro de uma organização. Eles têm muitos propósitos legítimos, como: filtragem de spam, filtrar e-mails e anexos maliciosos e adicionar uma assinatura corporativa no final de cada e-mail.
>
> Os eventos típicos tratados por um Agente de Transporte ocorrem quando o servidor de email envia ou recebe um email. Antes do evento ser efetivamente executado, os Agentes de Transporte são chamados e têm a possibilidade de modificar ou bloquear o email.

Sendo assim, percebe-se que o Agente de Transporte é um serviço natural e extremamente útil do *Microsoft Exchange*, contudo o *malware* se utiliza de tal serviço para atuações maliciosas, como pode ser ilustrado de forma mais claro pela imagem abaixo.

Figura 3 - Contaminação do Agente de Transporte.



Fonte: Faou (2019).

Porém para realização de tal feito, se faz necessário que o atacante consiga adentrar nessa estrutura. Tal processo de instalação ocorre através invasores que colocam um executável na pasta Exchange localizada na pasta Arquivos de Programas. Esta primeira etapa requer privilégios administrativos. Em seguida, eles executam o *script*, como mostrado na Figura 4 para registrar a DLL como Agente de Transporte.

Esta segunda etapa é necessária antes que o malware comece a receber eventos do Exchange.

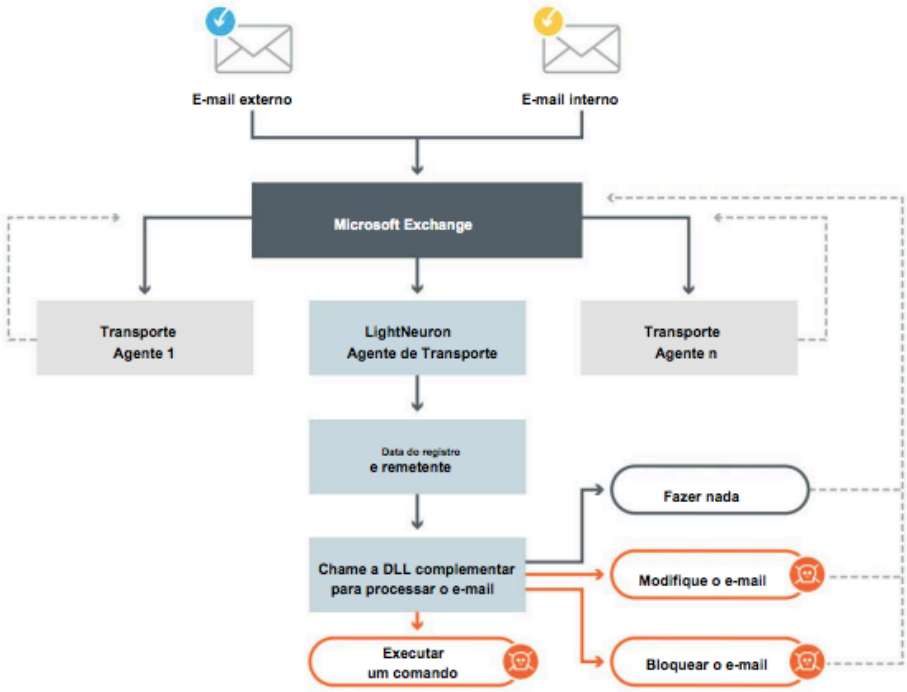
Figura 4 – Registro do DLL

```
Install-Transportagent -Name "Security Interop Agent" -AssemblyPath "c:\program
    files\microsoft\Exchange Server\v15\bin\Microsoft.Exchange.Security.Interop.dll" -
    TransportAgentFactory Microsoft.Exchange.Security.Interop.SecurityInteropAgentFactory
Install-Transportagent -Name "Content Filter Agent" -AssemblyPath "c:\program
    files\microsoft\Exchange Server\v15\bin\Microsoft.Exchange.Security.Interop.dll" -
    TransportAgentFactory Microsoft.Exchange.Security.Interop.ContentFilterAgentFactory

Enable-TransportAgent -Identity "Security Interop Agent"
Get-TransportAgent -Identity "Security Interop Agent"
Enable-TransportAgent -Identity "Content Filter Agent"
Get-TransportAgent -Identity "Content Filter Agent"

Get-TransportAgent
```

Fonte: Faou (2019).

De forma a facilitar entendimento, ressalta-se que uma DLL pode ser considerada parte de uma biblioteca para aplicativos do sistema operacional *Windows*, bem como para programação. Uma DLL contém um ou mais funções que são compiladas, vinculadas e armazenadas separadamente do aplicativos que os utilizam. Resumidamente, trata-se de um arquivo que contém código e dados que podem ser compartilhados entre vários programas no sistema *Windows*, tornando o desenvolvimento e a manutenção de software mais eficientes e modularizados (Takeuchi, 2002). Sendo neste caso partes contaminadas pelo atacante.

Figura 5 - Funcionamento do Turla LigthNeuron



Fonte: Faou (2019).

A Figura 5 demonstra o funcionamento do *Turla LigthNeutron* nas manipulações de e-mail, através de um Agente de Transporte malicioso. Desta forma, o atacante pode realizar diversas ofensivas, como modificações das mensagens a serem recebidas através do correio eletrônico, ou impedir que as mesmas sejam entregues. Contudo, o que determina o tipo de ataque a ser realizado é a configuração utilizada no DLL malicioso. Dessa forma, os atacantes tendem a customizar as configurações de acordo com o perfil da vítima selecionada.

De acordo com Faou (2019), em suas amostras analisadas, todos os endereços de e-mail sob determinada configuração de ataque pertenciam a uma organização específica. Nesse caso, monitoravam cerca de trinta endereços de e-mail diferentes, que provavelmente eram as pessoas sobre as quais estavam mais interessados em recolher informações.

Seguindo os estudos de Faou (2019), existem onze configurações diferentes implementados na DLL:

Tabela 1 – Configurações da DLL

Nome do Manipulador	Descrição
Block	Bloquear o e-mail
changeBody	Alterar o corpo do e-mail
changeTo	Alterar o destinatário do e-mail
changeSubject	Alterar o assunto do e-mail
command	Analise o anexo JPG/PDF, descriptografe e execute os comandos.
create	Crie um novo e-mail
Log	Registrar anexo de e-mail em LOG_OUTPUT
replace	Substitui o anexo
spam	Recria e reenvia o e-mail do servidor Exchange para ignorar o filtro de spam
Stat	Registrar de, data, até, assunto em STAT_PATH em formato CSV
zip	Criptografa o email com RSA e armazene-o no caminho especificado por ZIP_FILE_NAME.

Fonte: Faou (2019).

Destaca-se também que a descontaminação do sistema atingido pelo *LightNeuron* não é uma tarefa fácil. A simples remoção dos arquivos maliciosos gerará grandes problemas ao funcionamento do *Microsoft Exchange*, impedindo que todos na organização enviem e recebam e-mails. Para possibilitar a remoção dos arquivos contaminados de forma segura, primordialmente o Agente de Transporte malicioso deve ser desabilitado. Outro ponto a se destacar é a necessidade da troca das senhas de todas as contas que possuem direitos administrativos no servidor comprometido. Caso contrário, os invasores poderão acessar o servidor novamente para comprometê-lo novamente (Faou, 2019).

Verificando algumas das técnicas utilizadas pelo *Neuron* e como o mesmo conseguiu infectar um sistema sólido como do *Microsft Exchange*, torna-se perceptível, o porquê do mesmo ser um dos *malwares* mais bem-sucedidos do grupo *Turla*.

Com esse breve estudo do grupo *Turla*, pode-se perceber a grande eficiência em que infecções cibernéticas podem trazer ao contexto de conflitos internacionais. De maneira eficiente, o grupo conseguiu adentrar no sistema de e-mail, de forma em que até sua retirada trouxesse um grande malefício a estrutura do sistema. Vale salientar que no decorrer do período em que esta organização esteve infiltrada nos mais diversos países, a mesma teve a possibilidade de realizar diversas ações de espionagem e de coletar várias informações sensíveis dos setores alvos.

2.4 *Stuxnet*

2.4.1 Cenário

No que se refere a ataques a infraestruturas críticas, pode-se destacar o *malware* conhecido como *Stuxnet*, um dos maiores exemplos ocorridos na história. Considerado do tipo *worm*, desenvolvido especificamente para afetar infraestruturas críticas, mais precisamente os sistemas de controle industrial das usinas de enriquecimento de Urânio do Iran. Até hoje não se sabe a origem do ataque, porém devido à complexidade dos recursos utilizados no ataque e do nível de conhecimento necessário ao atacante do sistema sobre o alvo, acredita-se que o ataque tenha partido de uma ou mais nações e não de um *hacker* individual.

Tal ataque demonstra um grande nível de preparação pois para sua realização foi necessária uma série de ações que possibilitassem a introdução do *malware* ao sistema iraniano. A princípio seria necessário que os atacantes obtivessem acesso ao sistema de controle industrial (ICS) e pelo código em controladores lógicos programáveis (PLCs) que opera o ICS. Esses documentos de design podem ter sido roubados por alguém interno ou até mesmo recuperados por uma versão anterior do *Stuxnet* ou outro binário malicioso. Assim que os invasores tivessem os documentos de projeto e o conhecimento potencial do ambiente de computação da instalação, eles desenvolveriam a versão mais recente do *Stuxnet*. Cada recurso do *Stuxnet* foi implementado por um motivo específico e com o objetivo final de potencialmente sabotar o ICS (Falliere et al., 2010).

Contudo, para infectar o alvo, o *Stuxnet* precisaria ser introduzido no ambiente alvo. Isto pode ter ocorrido ao infectar um terceiro voluntário ou desconhecido, como um empreiteiro que talvez tenha tido acesso às instalações, ou uma pessoa interna. A infecção original pode ter sido introduzida por uma unidade removível.

Segundo Falliere et al. (2010), os ocorridos seguiram a seguinte linha cronológica de eventos:

Tabela 2: Cronologia de Eventos

Data	Evento
20 de novembro de 2008.	Descobriu-se que a variante Trojan.Zlob usa a vulnerabilidade LNK identificada apenas posteriormente no Stuxnet.
Abril, 2009.	A revista de segurança Hakin9 divulga detalhes de uma vulnerabilidade de execução remota de código no serviço Printer Spooler. Posteriormente identificado como MS10-061.
Junho de 2009.	Amostra mais antiga do Stuxnet vista. Não explora MS10-046. Não possui arquivos de driver assinados.

25 de janeiro de 2010.	Driver Stuxnet assinado com um certificado válido pertencente à Realtek Semiconductor Corps.
Março de 2010.	Primeira variante do Stuxnet a explorar o MS10-046.
17 de junho de 2010.	Virusblokada relata W32.Stuxnet (denominado RootkitTmphider). Relata que está usando uma vulnerabilidade no processamento de arquivos de atalhos/.lnk para propagação (posteriormente identificada como MS10-046)
13 de julho de 2010.	A Symantec adiciona detecção como W32.Temphid (anteriormente detectado como Cavalo de Tróia).
16 de julho de 2010.	A Microsoft emite um comunicado de segurança para "Vulnerabilidade no shell do Windows pode permitir a execução remota de código (2286198)" que cobre a vulnerabilidade no processamento de arquivos de atalhos/.lnk.
17 de julho de 2010.	A Eset identifica um novo driver Stuxnet, desta vez assinado com um certificado da JMicron Technology Corp
19 de julho de 2010.	A Siemens informa que está investigando relatos de malware infectando sistemas Siemens WinCC SCADA. A Symantec renomeia a detecção para W32. Stuxnet.
20 de julho de 2010.	A Symantec monitora o tráfego de comando e controle do Stuxnet
22 de julho de 2010.	Verisign revoga o certificado JMicron Technology Corps.
2 de agosto de 2010.	A Microsoft emite o MS10-046, que corrige a vulnerabilidade de atalho do Windows Shell.
6 de agosto de 2010.	A Symantec relata como o Stuxnet pode injetar e ocultar código em um PLC afetando sistemas de controle industrial.
14 de setembro de 2010.	A Microsoft lança o MS10-061 para corrigir a vulnerabilidade do spooler de impressora identificada pela Symantec em agosto A Microsoft relatou duas outras vulnerabilidades de escalonamento de privilégios identificadas pela Symantec em agosto
30 de setembro de 2010.	Symantec apresenta no Virus Bulletin e lança análise abrangente do Stuxnet.

Fonte: Falliere et al., 2010.

2.4.2 Estrutura *Stuxnet*

Segundo Falliere et al. (2010), o coração do *Stuxnet* consiste de um grande arquivo DLL, que contém uma grande quantidade de "*exports*[9]" e recursos. O componente *dropper*[10] do *Stuxnet* é um programa *wrapper*[11] que contém todos os componentes acima armazenados dentro de si em uma seção chamada "*stub*[12]". Esta seção de esboço é essencial para o funcionamento do *Stuxnet*.

Quando a ameaça é executada, o wrapper extrai o arquivo .dll da seção *stub*, mapeia-o na memória como um módulo e chama uma das exportações. Um ponteiro para a seção *stub* original é passado para esta exportação como parâmetro. Esta exportação, por sua vez, extrairá o arquivo .dll da seção stub, que foi passada como parâmetro, mapeá-lo-á na memória e chamará outra exportação diferente de dentro do arquivo .dll mapeado. O ponteiro para a seção *stub* original é novamente passado como parâmetro (Falliere et al., 2010).

Segundo Falliere et al. (2010), o arquivo .dll contém todo código para controlar o *worm*, cada tipo configuração desse dll tem uma finalidade de controle diferente. A forma de exportação escolhida influenciará na técnica de disseminação a ser utilizada, sendo fruto do estudo as seguintes formas de configuração:

Tabela 3: Configurações do Stuxnet

Configuração	Função
1	Infecta unidades removíveis conectadas, inicia o servidor RPC
2	Hooks APIs para infecções de arquivos de projeto da Etapa 7
4	Chama a rotina de remoção (exportação 18)
5	Verifica se a ameaça está instalada corretamente
6	Verifica informações de versão
7	Exportação de chamadas 6

[9] Capacidade de um sistema, aplicativo, módulo ou biblioteca de disponibilizar funções, variáveis ou recursos para uso por outros programas ou componentes.

[10] Parte de um software malicioso que tem a função de baixar e instalar outros componentes ou partes de um malware em um sistema de computador ou dispositivo.

[11] Software ou componente que envolve ou envolve outro programa, biblioteca, serviço ou recurso, geralmente com o objetivo de fornecer uma interface mais amigável, facilitar a integração.

[12] Comumente usados em programação, teste de software e integração de sistemas para várias finalidades.

9	Atualiza-se a partir de projetos infectados da Etapa 7
10	Atualiza-se a partir de projetos infectados da Etapa 7
14	Etapa 7 rotina de infecção de arquivo de projeto
15	Ponto de entrada inicial
16	Instalação principal
17	Substitui a DLL da Etapa 7
18	Desinstala o Stuxnet
19	Infecta unidades removíveis
22	Rotinas de propagação de rede
24	Verifique a conexão com a Internet
27	Servidor RPC
28	Rotina de comando e controle
29	Rotina de comando e controle
31	Atualiza-se a partir de projetos infectados da Etapa 7
32	Igual a 1

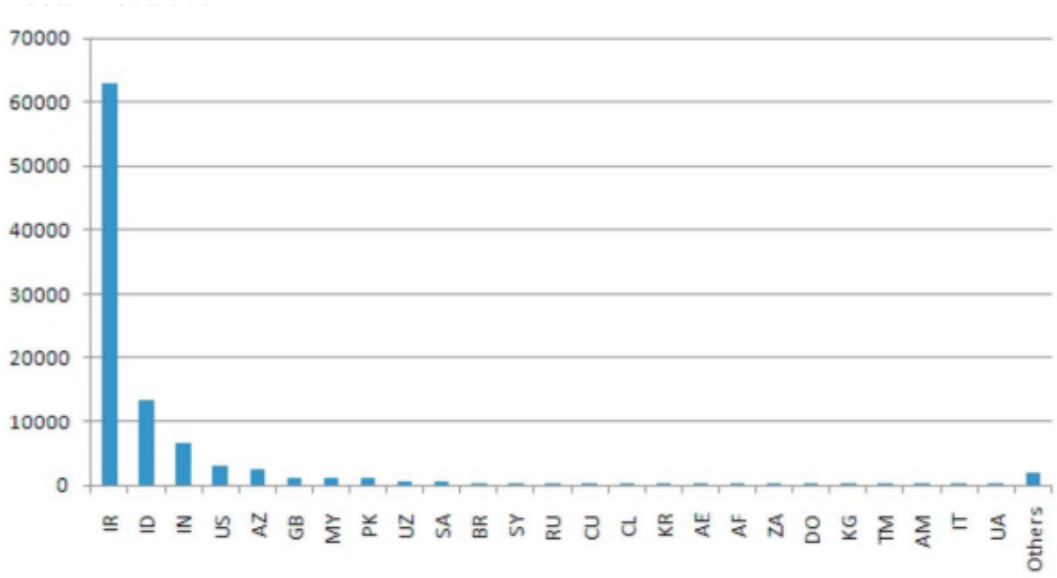
Fonte: Falliere et. al., 2010.

2.4.3 Estatísticas de atuação ao longo dos anos

A Figura 6 mostra a quantidade de *hosts* (dispositivos individuais que compõem uma rede e que podem se comunicar entre si), infectados em 29 de setembro de 2010. Além disso, a imagem foi gerada com base em informações obtidas por um sistema de monitoramento gerado pela *Symantec* para identificar o tráfego de computadores infectados. O sistema identificou apenas o tráfego de comando e controle de computadores que conseguiam se conectar aos servidores C&C. Os dados enviados de volta aos servidores C&C são criptografados e inclui dados como endereço IP interno e externo, nome do computador, versão do sistema operacional e se ele está executando o *software* de controle industrial *Siemens SIMATIC Step* 7[13] (Falliere et al., 2010).

13 *Softwares* de programação de automação industrial mais utilizados no mundo.

Figura 6- *Hosts* Infectados



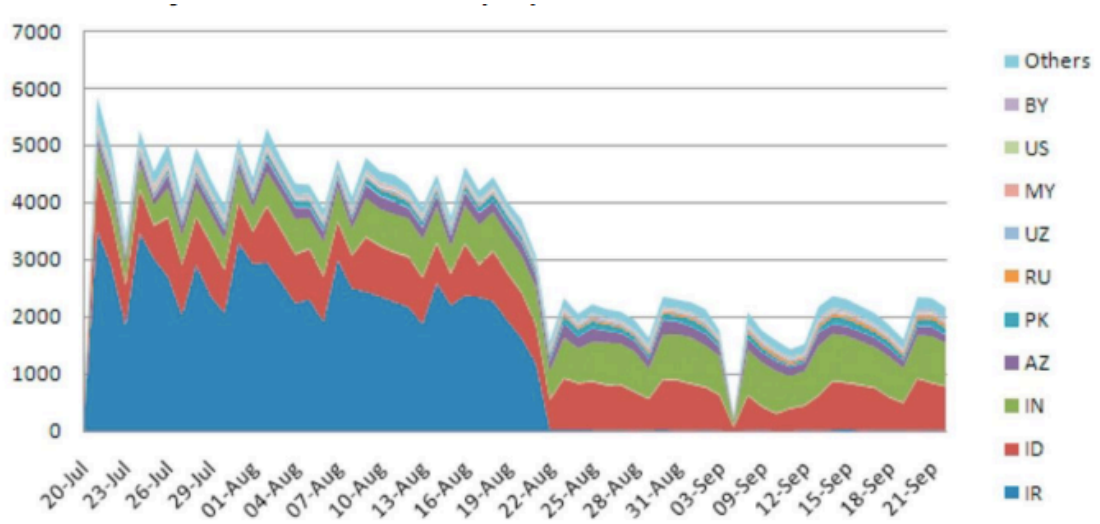
Fonte: Falliere et. al., 2010.

Embora os invasores pudessem controlar o *Stuxnet* com um servidor de comando e controle, como mencionado anteriormente, era improvável que o computador principal tivesse acesso de saída à Internet. Assim, todas as funcionalidades necessárias para sabotar um sistema foram incorporadas diretamente no executável do *Stuxnet*. As atualizações deste executável seriam propagadas por toda a instalação através de um método *peer-to-peer*[14] estabelecido pelo Stuxnet (Falliere et al., 2010).

O gráfico da Figura 7 demonstra a taxa de infecção do *Stuxnet* de novos IPs por país.

14 Modelo de rede de computadores em que os dispositivos, como computadores, servidores, ou outros dispositivos, se comunicam diretamente entre si, sem a necessidade de um servidor centralizado.

Figura 7- Concentração de ataques por país



Fonte: Falliere et. al., 2010.

A concentração de infecções no Irã provavelmente indica que este foi o alvo inicial das infecções e foi onde as infecções foram inicialmente semeadas. Embora o *Stuxnet* seja uma ameaça direcionada, o uso de uma variedade de técnicas de propagação fez com que o *Stuxnet* se espalhasse além do alvo inicial. É provável que essas infecções adicionais sejam "danos colaterais" – efeitos colaterais não intencionais da metodologia promíscua de propagação inicial utilizada pelo *Stuxent*. Embora as taxas de infecção provavelmente caiam à medida que os usuários corrijam seus computadores contra as vulnerabilidades usadas para propagação, *worms* dessa natureza normalmente continuam a ser capazes de se propagar por meio de computadores inseguros e sem correção (Falliere et al., 2010).

2.4.4 Técnicas de disseminação

A infecção do *Stuxnet* ocorre através da porta USB de um microcomputador, onde um dispositivo *flash* precisa ser conectado carregando o código malicioso. Após a infecção do primeiro computador, o *Stuxnet* se propaga pelos demais computadores interligados em busca de seu sistema alvo. O *Stuxnet* somente infectará três computadores de uma determinada unidade *flash* contaminada, sendo codificado para parar de se espalhar após 24 de junho de 2012. (Mueller, 2012). Após o terceiro computador infectado ele se auto apaga da unidade *flash*. No caso das Usinas de Natanz, as unidades flash infectadas podem ter sido introduzidas nos computadores de

controle por meio de trabalhadores contratados externamente para trabalhar na fábrica. (Mueller; Yadegari, 2012)

A propagação ocorre através da rede *LAN*, na qual os computadores da empresa encontram-se conectados. O *Stuxnet* é capaz de se replicar na maioria das vezes, através de vulnerabilidades de *zero-day* encontradas no sistema operacional *Windows*. Os mecanismos de propagação do *Stuxnet* são todos baseados em *LAN* e, portanto, o alvo final deve ser considerado em localização próxima na rede local aos alvos iniciais. (Falliere et al., 2010). Os computadores nos quais os sistemas de Controle são instalados não possuem contato com internet, portanto a disseminação somente poderia correr por meio de dispositivo flash ou pela própria rede *LAN*. Após a disseminação do *Stuxnet* através da rede, o worm verifica se a máquina onde ele se encontra faz parte do sistema alvo do ataque, no caso, ele verifica se o computador possui o software *SIMATIC Step* 7, sistema desenvolvido pela *Siemens* (Empresa Alemã de infraestrutura e tecnologia) para controle das centrífugas das usinas de enriquecimento de Urânio do Iran. Uma vez em funcionamento, o *Stuxnet* compromete a máquina alvo.

Segundo relata Falliere et al. (2010), A configuração 22 do DLL é responsável pela maioria das rotinas de propagação de rede que o *Stuxnet* utiliza. Esta exportação cria uma classe "*Network Action*" que contém 5 subclasses. Cada subclasse é responsável por um método diferente de infectar um host remoto. As funções das 5 subclasses são:

- **Comunicação ponto a ponto** - O componente P2P funciona através da instalação de um servidor e cliente RPC (Chamada Remota de Procedimento). Quando a ameaça infecta um computador, ela inicia o servidor RPC e escuta conexões. Qualquer outro computador comprometido na rede pode se conectar ao servidor RPC e perguntar qual versão da ameaça está instalada no computador remoto. Se a versão remota for mais recente, o computador local fará uma solicitação para a nova versão e se atualizará com ela. Se a versão remota for mais antiga, o computador local preparará uma cópia de si mesmo e a enviará ao computador remoto para que ele possa se atualizar. Desta forma, uma atualização pode ser introduzida em qualquer computador comprometido em uma rede e eventualmente se espalhará para todos os outros computadores comprometidos.

- **Infectando computadores *WinCC* -** Esta classe é responsável por conectar-se a um servidor remoto executando o *software* de banco de dados *WinCC* (*software* de supervisão e controle industrial desenvolvido pela Siemens). Quando encontra um sistema executando este software, ele se conecta ao servidor de banco de dados usando uma senha codificada no software *WinCC*. Depois de conectado, ele executa duas ações. Primeiro, o *Stuxnet* envia código SQL malicioso ao banco de dados que permite que uma versão do *Stuxnet* seja transferida para o computador que executa o *software WinCC* e o executa, infectando assim o computador que está executando o banco de dados *WinCC*. Em segundo lugar, o *Stuxnet* modifica uma visualização existente, adicionando código que é executado sempre que a visualização é acessada.

- **Propagação através de compartilhamentos de rede**- O *Stuxnet* também pode se espalhar para compartilhamentos de rede disponíveis por meio de um trabalho agendado ou usando o *Windows Management Instrumentation* (infraestrutura de gerenciamento de sistemas da *Microsoft* que fornece informações detalhadas sobre o estado e a configuração de dispositivos e aplicativos em computadores Windows). O *Stuxnet* enumerará todas as contas de usuário do computador e do domínio e testará todos os recursos de rede disponíveis usando o *token* de credencial do usuário ou operações WMI com o *token* explorer.exe para copiar a si mesmo e executar no compartilhamento remoto.

- **Propagação através da Vulnerabilidade de zero-day do *spooler* de impressão-** Esta vulnerabilidade permite que um arquivo seja gravado na pasta %System% de máquinas vulneráveis. O código real para realizar o ataque é armazenado no recurso 222; esta exportação carrega a DLL armazenada naquele recurso e prepara os parâmetros necessários para executar o ataque, ou seja, um endereço IP e uma cópia do *worm*, e então chama a exportação da DLL carregada. Usando essas informações, o *Stuxnet* é capaz de copiar a si mesmo para computadores remotos por meio do *Spooler* de impressora e, em seguida, executar a si mesmo. Winsta.exe pode conter várias cópias do *Stuxnet* e ficar anormalmente grande.

- **Propagação através da Vulnerabilidade do serviço MS08-067 *Windows Server-*** o *Stuxnet* também explora o MS08-067, que é a mesma vulnerabilidade utilizada pelo W32.Downadup. MS08- 067 pode ser explorado conectando-se através de SMB e enviando uma *string* de caminho malformada que permite a execução arbitrária. O *Stuxnet* usa essa vulnerabilidade para se copiar em computadores remotos sem correção.

De acordo com Falliere et al. (2010), além das propagações em rede, um dos principais métodos de propagação que o *Stuxnet* usa é copiar-se para unidades removíveis inseridas. Os sistemas de controle industrial são comumente programados por um computador *Windows* que não está conectado à rede e os operadores geralmente trocam dados com outros computadores usando unidades removíveis. O *Stuxnet* usou dois métodos para se espalhar de e para unidades removíveis – um método usando uma vulnerabilidade que permitia a execução automática ao visualizar a unidade removível e o outro usando um arquivo autorun.inf.

O *Stuxnet* não é prejudicial aos usuários comuns, pois seu objetivo é modificar os PLCs fabricados pela Siemens. Inicialmente o *Stuxnet* monitora a operação da máquina infectada, após isso ele utiliza as informações reunidas para tomar o controle das centrifugas, fazendo-as operar de forma incorreta, de maneira a conduzir o sistema à falha. Durante a ação, o *Worm* envia falsos *feed-back* para os operadores do sistema, fazendo-os acreditar que o funcionamento das centrifugas encontra-se em estado normal. No contexto do ataque realizado as usinas do Iran, o ataque pode ser considerado bem-sucedido, uma vez que ele foi capaz de destruir 1.000 centrifugas das usinas de Natanz, o que representava 11% da capacidade do país na época do ataque (Mueller; Yadegari, 2012).

Com esse breve estudo sobre o *Stuxnet* é visível a grande importância desse *malware* para o contexto das guerras travadas por ataques cibernéticos. Aumentando sobremaneira a probabilidade que os autores de *malware*, sejam eles estados-nação ou entidades menores, perpetrarem ataques semelhantes no futuro. O *Stuxnet* provou que tais ataques cibernéticos fora da rede são possíveis, aumentou o conhecimento sobre eles e o interesse por entre as entidades maliciosas, além de conceder uma base de código sofisticada para atacantes estudarem e modificarem.

3. METODOLOGIA

O presente estudo de caso busca trazer à tona os perigos da utilização de redes de comunicação para interligar controladores e plantas físicas em meios navais. Além de motivar as estruturas militares a adaptação aos novos paradigmas tecnológicos, visto que a integração dos sistemas é uma nova realidade para quais as belonaves tendem a caminhar

Neste contexto, têm sido realizados estudos com o objetivo de explorar vulnerabilidades e propor soluções de segurança para sistemas ciber-físicos. Neste trabalho será proposto um ataque para manipulação dos sistemas de controles e adaptação as plantas dos meios navais, além de possíveis formas de mitigação destas ofensivas para realizar. Para tal foi realizada uma pesquisa de forma exploratória utilizando como meio referências bibliográficas.

3.1 Classificação de pesquisa

3.1.1 Quanto aos fins

Segundo Gil (2002), a verificação exploratória é feita em área na qual existe baixa informação acumulada e sistematizado. Pode-se dizer que estas pesquisas têm como objetivo principal o aprimoramento de ideias ou a descoberta de intuições. eu planejamento é, portanto, bastante flexível, de modo que possibilite a consideração dos mais variados aspectos relativos ao fato estudado. Na maioria das vezes, essas pesquisas envolvem: levantamento bibliográfico, entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado e análise de exemplos que auxiliem o entendimento.

Dessa forma, a presente pesquisa enquadra-se como exploratória. Uma vez que, por meio do levantamento de informações prévias sobre a estrutura de sistemas de controle industriais, sistemas de controle industriais a bordo de navios, ataques ciber-cíneticos e arquitetura de ataques furtivos baseados em perda de dados foi possível realizar uma análise de como ofensivas cibernéticas podem representar uma ameaça a um Estado e seu Poder Marítimo.

3.1.2 Quanto aos meios

Quanto aos meios, utilizou-se a pesquisa bibliográfica, através da revisão de literatura disponível sobre o tema exposto o qual tem como seu maior objetivo estabelecer a base teórica da pesquisa, incluindo suas ferramentas analíticas.

> A pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos. Embora em quase todos os estudos seja exigido algum tipo de trabalho dessa natureza, há pesquisas desenvolvidas exclusivamente a partir de fontes bibliográficas. Boa parte dos estudos exploratórios pode ser definida como pesquisas bibliográficas. As pesquisas sobre ideologias, bem como aquelas que se propõem à análise das diversas posições acerca de um problema, também costumam ser desenvolvidas quase exclusivamente mediante fontes bibliográficas (Gil, 2002).

4. ESTUDO DE CASO

4.1 Contexto

Os ataques cibernéticos podem assolar diversos setores da economia de um país e alvos ligados a estrutura marítima podem ser extremamente relevantes para esses possíveis atacante, devido a forte representatividade econômica que este setor possui. A indústria marítima representa 90% das trocas comerciais realizadas em todo o mundo, onde dele dependem as cadeias de abastecimento dos principais setores produtivos. Por isso, o setor marítimo, como parte vital da economia global deve ser protegida contra ameaças e ataques cibernéticos. Um incidente cibernético pode levar a um grande desastre ambiental ou económico, podendo mesmo causar a perda de vidas humanas. Dessa forma, o setor marítimo precisa imergir em um processo de adaptação ao novo ambiente exigido pelas tecnologias de informação (cria, processa, armazena, informação, etc.), e integra tecnologia operacional (monitores, controle, etc.) com o objetivo de otimizar os processos de gestão (Alcaide et al., 2019.).

Contudo, Freire et al., (2023) relata que existe um grande crescimento do setor marítimo, fruto do uso crescente da tecnologia da Indústria 4.0, integrando muitos de seus sistemas autônomos em sistemas ciber- físicos complexos.

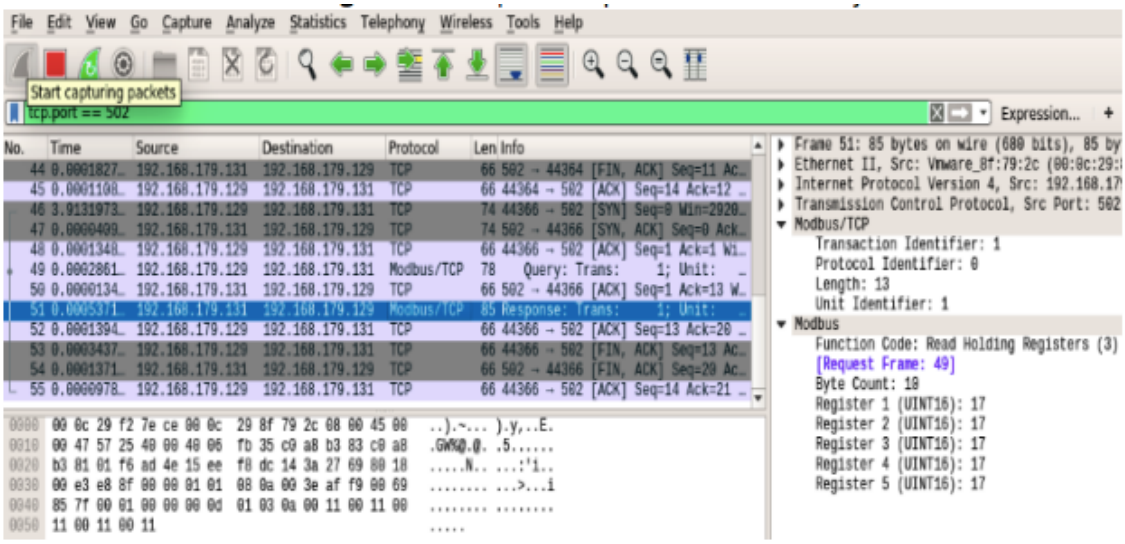
A partir desse pensamento, o presente trabalho apresentará um modelo de ataque que terá como seu objetivo interferir em um sistema de controle de um navio, para isso serão detalhadas algumas etapas para que tal feito ocorra com sucesso. Inicialmente será discorrido sobre a infraestruturas e as vulnerabilidades encontradas nos sistemas de controle utilizados na indústria marítima. Posteriormente será apresentado metodologias para realização da identificação da cadeia de suprimentos e introdução do vetor de ataque inicial e como o a cibernético empregado realizaria um movimento lateral para alcançar a estrutura do alvo principal. Finalmente serão apresentados os mecanismos do ataque passivo de identificação do sistema, que por sua vez permite uma maior adaptabilidade do modelo de ataque a diferentes plantas industriais.

4.2 Infraestrutura e Vulnerabilidade dos Sistemas de Controle

Os sistemas controlados por rede (NCS) tem trazido consigo grandes benefícios a indústria marítima, as tripulações podem ser mais reduzidas pela automação dos sistemas principais do navio. Essa automação é possível devido à utilização de modernos protocolos *Real-Time Ethernet* (RTE) que atendem demandas de alta amostragem e baixa latência, como, por exemplo, o protocolo PROFINET amplamente utilizado na indústria naval (Freire et al., 2023).

No entanto, o RTE tem consigo alguns problemas de segurança, o principal é a falta de autenticação entre os atores dos sistemas de automação e controle, abrindo as portas da rede para qualquer dispositivo malicioso que possa se comportar como quaisquer outros participantes (Ferrari et al., 2021). Os dispositivos de controle, a partir dessa integração com os protocolos do switch TCP/IP, possuem IP e podem ser acessados remotamente, podendo também ser facilmente interpretados pois os protocolos de controle e automação encapsulado em datagramas transmitem informações em claro (Ackerman, 2021). A Figura 8 apresenta uma captura a partir do software *Wireshark* de pacotes de comunicação do protocolo *RTE Modbus*.

Figura 8 - *Wireshark* capturando pacotes



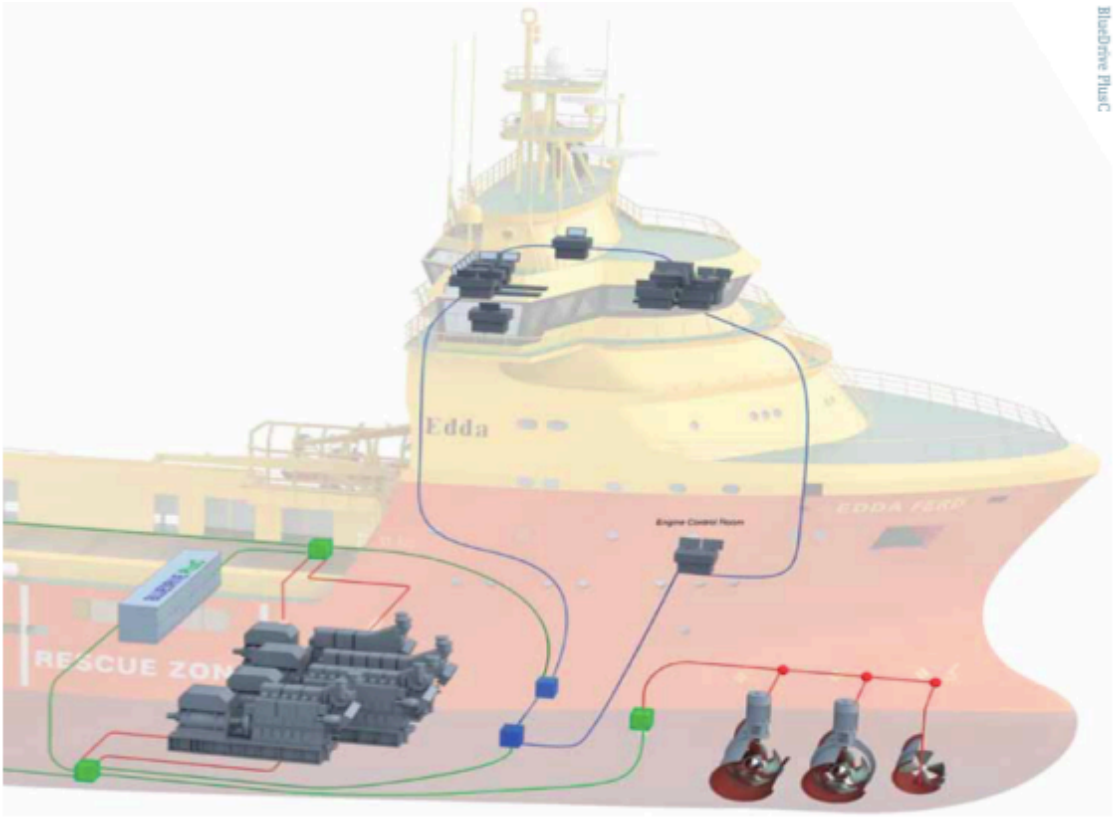
Fonte: Arckeman 2021.

Dessa forma é perceptível que muitos dos OT(Tecnologia Operacional) implementados em navios modernos não foram originalmente projetados para serem integrados a sistemas de TI, carecendo de mecanismos fundamentais de defesa cibernética, como autenticação e criptografia. Essas vulnerabilidades foram amplamente exploradas pelos invasores, com o MTS(Sistema de Transporte Marítimo**)** sofrendo ameaças crescentes visando principalmente a direção de navios, navegação, propulsão, carga e sistemas de energia (Freire et al., 2023).

Contudo, os sistemas de controle industrial fundamentados no protocolo *PROFINET* tem apresentado sua grande eficácia, mesmo que os inconvenientes relacionados a segurança ainda se mantenham. A Figura 9 demonstra um recente sistema de propulsão de navios que se utiliza do protocolo *PROFINET*, conhecido como sistema *BlueDrive PlusC*, idealizado pela Siemens (Siemens, 2017).

Na Figura 9, a malha de controle do sistema de propulsão onde a malha em vermelho corresponde a alimentação dos motores, a malha azul corresponde a linha de fibra óptica Ethernet e a malha em vermelho representa as ligações *PROFINET* (SIEMENS, 2017). Destaca-se que esse sistema tem consigo uma implementação holística para navios diesel-elétricos, juntamente com o sistema de controle da propulsão e da geração de energia. O sistema tem a capacidade de diminuir o uso de combustível em até 19% se comparado com os sistemas tradicionais. Além disso existe a possibilidade do aumento do ciclo de vida dos equipamentos e diminuição da emissão de gases por meio de uma utilização eficiente do diesel (Freire et al., 2023).

Figura 9 - Sistema de controle integrado baseado no protocolo PROFINET



Fonte: Siemens 2017.

4.3 Projeto de ataque

Normalmente, os ataques são realizados visando algum lucro a ser obtido. Infelizmente, esse lucro vem aumentando nos últimos anos devido às mudanças no cenário industrial. Na verdade, algumas características das plantas industriais que dificultavam a realização de ataques estão mudando, reduzindo o investimento necessário para realizar um ataque com sucesso. Por exemplo, embora as redes RTE estivessem frequentemente ligadas e isoladas da Internet, dificultando o acesso físico às mesmas, com a Indústria 4.0 este isolamento já não existe. Além disso, as habilidades e o conhecimento exigidos dos invasores sobre a operação de sistemas de automação industrial em tempo real estão se tornando menos rigorosos devido ao acesso fácil e gratuito à documentação (o poder computacional também está ficando mais barato). Finalmente, embora o número de metas possíveis fosse inferior em comparação com outros setores (por exemplo, empresas financeiras e de serviços), este número está agora a aumentando rapidamente (Ferrari et al., 2021).

De acordo com Alcaide et al. (2019), no setor marítimo e mais especificamente na navegação marítima, tem sido revelada a vulnerabilidade de determinados sistemas de navegação, onde os ciberataques introduzem sinais falsos que se sobrepõem à localização real dos navios ou representam emergências inexistentes. Estas circunstâncias são agravadas pelo aumento da utilização de tecnologia para controle de navegação, motores, cargas, entre outros. Assim como pela utilização de posicionamento dinâmico, interfaces navio-terra, controle de sistemas de propulsão ou abertura e fecho de cargas, válvulas, sistemas de embarque de passageiros. É necessário considerar que o fator humano desempenha um papel fundamental na eficácia dos ataques cibernéticos como um elemento significativo de vulnerabilidade para as empresas. Portanto, a principal barreira de qualquer instalação crítica e da própria embarcação é o seu pessoal e a sua prontidão e preparação contra-ataques cibernéticos.

Entretanto esse trabalho tenderá a detalhar os ataques cibernéticos relacionado aos sistemas de controle dos meios navais e possíveis consequências. O *malware* proposto para realização desse ataque terá como base dois princípios: avaliar os coeficientes da função de transferência da planta e capacidade de não ser percebido ou detectado (De Sá; Carmo; Machado, 2017).

4.3.1 Identificação da cadeia de suprimentos e introdução do vetor de ataque inicial

Segundo Freire et al. (2023), a etapa inicial pode ser considerado um tanto desgastante, pois consiste em uma fase de pesquisa através de técnicas de OSINT [15] , utilizando informações publicamente disponíveis, sobre a cadeia de suprimentos do alvo. Dessa forma, poderá se encontrar um bom vetor de iniciação, com o conhecimento dos seus fabricantes, seus protocolos de comunicação utilizados entre outras informações.

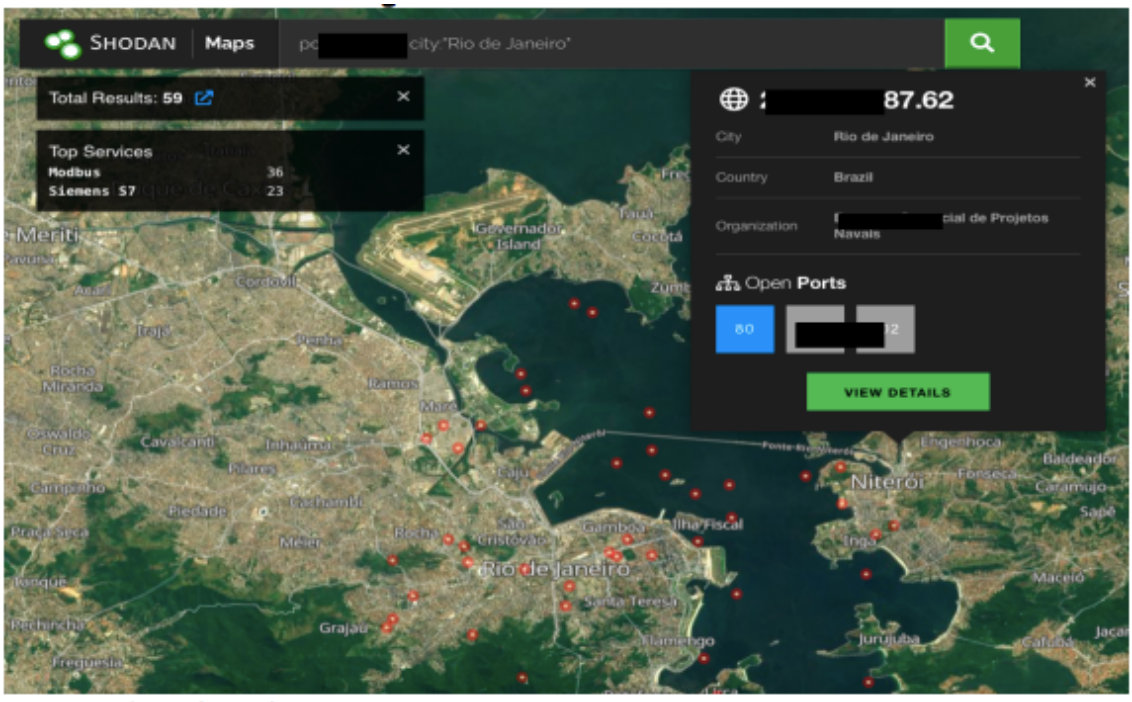
> Por exemplo, se o alvo escolhido empregar geradores Siemens, uma simples busca na internet permite verificar que poucas empresas especializadas prestam serviços de manutenção para esse tipo de equipamento em uma cidade como o Rio de Janeiro. Dessa forma, é possível delimitar o escopo dos possíveis alvos que serão empregados como vetor

15 Processo de coleta, análise e interpretação de informações obtidas a partir de fontes de acesso público.

> inicial do ataque. A partir dessa identificação, se inicia a etapa de levantamento da cadeia de clientes dessa empresa de manutenção que permitirá a infiltração do artefato cibernético até o alvo principal (Freire et al., 2023).

A partir disso, ferramentas mais sofisticadas como Engenharia Social e *Spear Phishing* são utilizadas para mapear clientes vulneráveis desta empresa de manutenção que serão utilizados como vetor inicial de ataque. Para completar esta tarefa, o motor de busca *Shodan* é usado para pesquisar PLC de um determinado fabricante atendido pela empresa de manutenção escolhida.

Figura 10 - Demonstração *Shodan*



Fonte: Freire et al. 2023

Após descoberto o vetor inicial perfeito e contaminado a PLC do equipamento do engenheiro responsável por realizar manutenções na empresa alvo, a primeira fase do ataque esta completa. Tal sistemática de ataque se assemelha a utilizada pelo *Stuxnet* como forma de contaminar infraestruturas que estão a separadas por *air gap*. É importante destacar que o *payload* com a carga de ataque ficará inerte neste equipamento e só será ativado quando em contato com o sistema específico, que neste caso será a estrutura de sistema controle do gerador da empresa alvo (Freire et al., 2023).

Essa estratégia aproveita o fato de que o alvo principal geralmente possui uma segurança cibernética mais estruturada do que suas organizações parceiras com menos recursos. Então, torna-se mais fácil comprometer primeiro os pequenos (Freire et al., 2023).

4.3.2 Princípios do *Malware* escolhido e realização do ataque

Após o contato com o sistema de controle do alvo, o ataque volta a prosseguir, para a realização dessa manipulação o *malware* escolhido será o *Backtrack Search Optimization Algorithm* (BSA), um algoritmo evolutivo que utiliza as informações obtidas por gerações passadas – ou iterações – para realizar a busca de soluções para problemas de otimização. O algoritmo possui dois parâmetros que são ajustados empiricamente: o tamanho de sua população P; e ÿ, descrito que estabelece a amplitude dos movimentos dos indivíduos de P. O parâmetro ÿ deve ser ajustado visando atribuir ao algoritmo boas capacidades de exploração e aproveitamento (De Sá; Carmo; Machado, 2017). Dessa forma, ele irá para primeiro inferir as funções da planta do gerador e, em seguida, identificar a melhor solução de ataque (Freire et al., 2023).

Se a entrada i(k) e a saída o(k) de um dispositivo do NCS forem conhecidas, o modelo desse dispositivo pode ser avaliado aplicando o i(k) conhecido num modelo estimado, que deve ser ajustado até à sua a produção estimada oˆ(k) convergir para o(k). Neste sentido, o BSA é utilizado para ajustar interativamente o modelo estimado, minimizando uma função de aptidão específica, até que o modelo estimado convirja para o modelo real do dispositivo real, que pode ser um controlador ou uma planta do NCS (De Sá; Carmo; Machado, 2017).

Para realização do ataque o BSA pode se utilizar de duas metodologias, a primeira seria degradar um serviço físico através da indução de um *overshoot* durante a resposta transitória de uma planta. Os *overshoots*[16] consistem em picos ocorridos quando o sistema excede o valor alvo durante a resposta transitória, podem causar estresse e possivelmente danificar sistemas físicos, como sistemas mecânicos, químicos e eletromecânicos. Além disso, por ocorrerem em um curto período de tempo, os

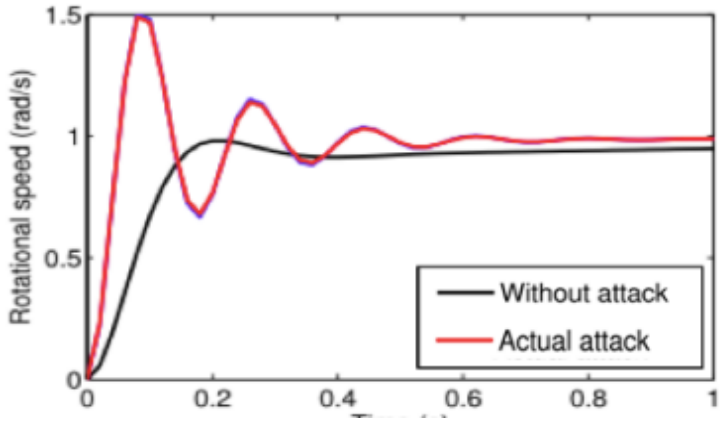
[16] Extensão pela qual uma resposta excede o valor de pico desejado em uma resposta transitória a uma mudança de entrada. É um fenômeno indesejado que ocorre em sistemas de controle quando o sistema responde exageradamente a uma mudança no sinal de entrada antes de se estabilizar.

overshoots são difíceis de serem percebidos por um observador humano (De Sá; Carmo; Machado, 2017).

A outra forma seria degradar o serviço da planta é causar nela um erro constante em estado estacionário, ou seja, produzir um erro constante quando t ÿ ÿ. Um erro de estado estacionário de baixa proporção, além de ser difícil de ser percebido por um observador humano, pode reduzir a eficiência do processo físico ou, ocasionalmente, estressar e danificar o sistema a médio/longo prazo (De Sá; Carmo; Machado, 2017).

Neste trabalho será utilizado o BSA para uma indução ao *overshoot* através da degradação no sistema através da derrubada de um número mínimo de frames da comunicação entre gerador e controlador (Freire et al., 2023) como ilustra a Figura 11. Ressalta-se também a necessidade que o ataque cause um efeito físico que não pode ser facilmente percebido ou identificado por um observador humano. O ataque deve modificar ligeiramente alguns comportamentos do sistema de forma a afetar fisicamente a planta, mas o efeito não deve ser facilmente perceptível ou que seja eventualmente confundido como consequência de outra causa raiz, diferente de um ataque. Visando que o *malware* possa persistir no sistema causando seus malefícios sem ser detectado (De Sá; Carmo; Machado, 2017).

Figura 11- Ataque de degradação de serviço

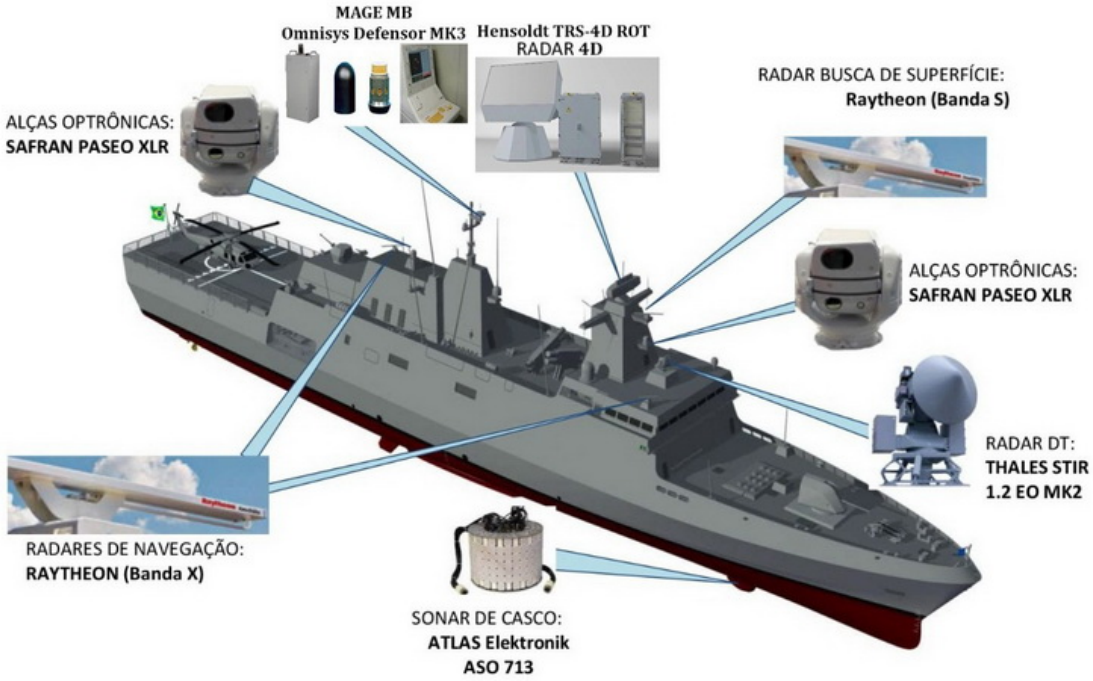


Fonte: De Sá, Carmo e Machado (2017).

Tal ataque visa diminuir de forma meticulosa o MTBF (*Mean Time Between Failures*) com a intenção de trazer problemas na distribuição da energia 440v. Dessa

forma, aumentando a probabilidade de causar degradação em sensores primordiais que dependem dessa energia a bordo (Ferrari et al., 2021).

Figura 12- Sensores de bordo dependentes da fonte 440V



Fonte: Adaptado de Caiafa (2020)

> A Figura 12 ilustra alguns dos sistemas que dependem dessa fonte de energia e podem ser severamente afetados em caso de perturbações de sua fonte de alimentação. Como os navios possuem mais de um gerador, sempre que um gerador afetado pelo ataque for acionado, ele poderá danificar os sistemas que estejam em operação no momento, potencialmente comprometendo a operacionalidade do meio. Dessa forma, o ataque proposto pode causar danos consideráveis, tanto no curto prazo (danificando importantes sensores do navio) quanto no longo prazo (reduzindo o MTBF do gerador) (Freire et al., 2023).

Contudo, segundo Ferrari et al. (2021) para que essa ofensiva seja possível e cumpra os seus resultados dentro de um sistema PROFINET, certas medidas devem ser adotadas. Ressalta-se que o protocolo emprega ciclos de amostragem curtos e estritamente repetitivos, além do emprego de *Timers Computer Operating Properly* (COP), que reduz a possibilidade de que a ofensiva seja bem-sucedida, pois esses podem disparar alarmes em caso de interrupção da troca de frames.

Sendo assim, de acordo com Ferrari et al. (2021), os seguintes requisitos devem ser cumpridos, ressalta-se que os passos estão representados na Figura 13, de forma a facilitar o entendimento do leitor:

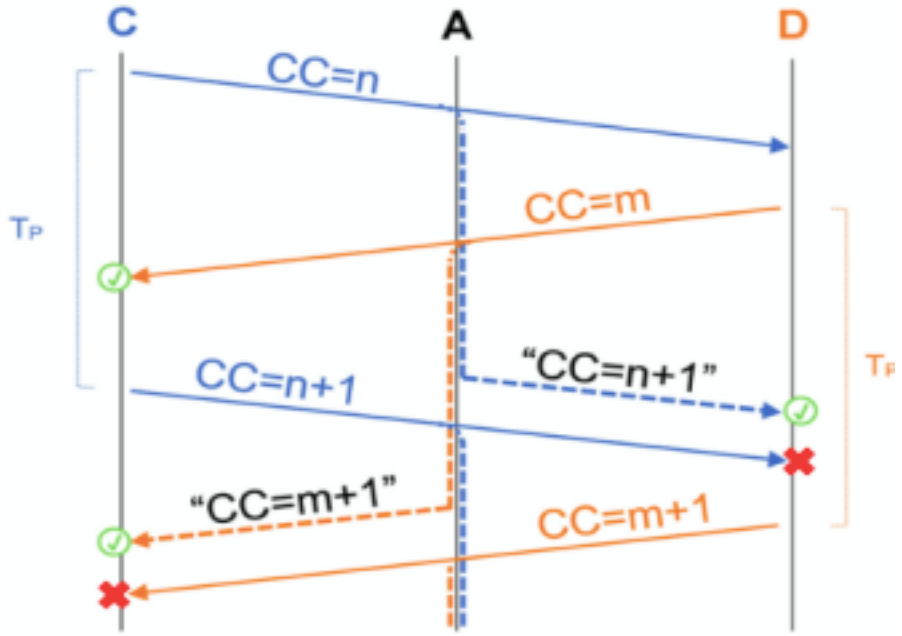
I) Durante o ciclo de comunicação, o artefato malicioso (A) emprega a técnica de ataque *Men in the Middle* (MitM4). Dessa forma, (A) recebe o frame de comunicação entre (C) e (D) que possui o valor do contador de ciclos (CC) igual a n;

II) O invasor A modifica a carga útil, de acordo com a lógica de degradação do serviço, aumentando o Contador de Ciclo do quadro para corresponder ao próximo valor esperado pelo destino do quadro (ou seja, o contador de ciclo para o ciclo n + 1).

III) De maneira semelhante, o *malware* envia novamente um frame modificado, agora com destino à (C), antes que o frame de (CC) igual a m+1 seja enviado por (D);

IV) O dispositivo alvo obtém o quadro modificado, ele usa-o como o frame do ciclo n+1 , descartando (ignorando) o original que será recebido posteriormente

Figura 13 - Ofensiva ao protocolo PROFINET



Fonte: Ferrari et al. (2021).

5. DISCUSSÕES SOBRE O ESTUDO DE CASO

Após exemplificado no estudo de caso acima, uma possível forma de ataque ao ICS de um navio, percebe-se que tal ataque pode também afetar meios militares. Os navios militares têm se tornado a cada dia mais dependentes de sistemas de tecnologia avançada para suas operações, incluindo navegação, comunicações, sistemas de armas e controles de engenharia. Ataques cibernéticos bem-sucedidos podem comprometer a funcionalidade desses sistemas, colocando em risco a segurança operacional.

Sendo assim, a capacidade de resistir a ataques cibernéticos é essencial para a resiliência estratégica. A dependência de tecnologia exige que as forças militares estejam preparadas para proteger suas operações em face de ciberataques.

Dessa forma, Freire et al. (2023) elucida algumas formas de defesa que poderiam ser implantadas visando dificultar as ofensivas de possíveis atacantes:

- Implementação de *Honeypot* PLC[17] com a mesma metodologia que utilizamos para armar um PLC;
- Implementação de *firewall*[18] industrial (IFW), especialmente projetado para lidar com redes OT de baixa latência;
- Uso de protocolos RTE mais avançados e mais seguro; e
- Sistema de detecção de intrusão e anomalia (IADS). Uso do aprendizado da máquina em uma perspectiva holística para monitorar o tráfego de rede industrial e processos físicos gerenciados, integrando ainda mais dispositivos heterogêneos a uma estrutura de detecção unificada adaptada para redes em tempo real de alta velocidade.

Contudo, vale ressaltar a necessidade do aumento da mentalidade de segurança dos tripulantes e dos mantenedores dos meios. Visto que nos diversos exemplos anteriormente relatados, ataques conseguem ser efetivos graças a estratégias de engenharia social. Dessa forma se faz necessário, diluir a falsa impressão de segurança

[17] Forma específica de *honeypot* que é projetada para atrair e detectar ataques direcionados a Controladores Lógicos Programáveis.

[18] Componente de segurança de rede ou *software* projetado para proteger uma rede de computadores ou dispositivo individual contra ameaças cibernéticas, como ataques, *malware* e acesso não autorizado.

em que os meios navais acreditam se encontrar, por estarem utilizando a estratégia air-gap.

6. CONCLUSÃO

A intersecção entre guerra cibernética e guerra tradicional é um aspecto complexo da segurança e estratégia militar no período atual. Com o constante avanço dos aparatos tecnológicos, a sociedade se torna mais interconectada, a importância da guerra cibernética como um componente crítico das operações militares não pode ser subestimada. Neste trabalho buscou-se explorar como essas duas esferas de conflito estão interligadas, destacando a importância de compreender as implicações desse relacionamento.

A guerra cibernética, em sua essência, é uma extensão da guerra tradicional. Ela amplia as capacidades militares, permitindo que as forças armadas conduzam operações de maneiras que anteriormente não eram possíveis. Em conflitos convencionais, a capacidade de realizar ataques cibernéticos bem-sucedidos pode fornecer uma vantagem estratégica significativa. Como tal, os militares em todo o mundo estão integrando a guerra cibernética em suas estratégias para complementar as operações tradicionais e proteger suas próprias redes e sistemas críticos.

Como demostrado na seção do trabalho que aborda o ataque do *Stuxnet*, a desestabilização da infraestrutura crítica, como sistemas de energia, telecomunicações e transporte, é uma das áreas-chave em que a guerra cibernética pode ter um impacto substancial. Ao perturbar ou desativar esses sistemas, as forças militares podem prejudicar gravemente a capacidade do inimigo de conduzir operações convencionais, assim como desestabilizar pilares da estrutura social da nação atingida. Além disso, a obtenção de informações de inteligência é fundamental em qualquer conflito, e a guerra cibernética oferece uma maneira eficaz de obter informações sensíveis e táticas do adversário como discorrido na seção sobre o grupo *Turla*.

No decorrer da seção que trata sobre o contexto político foi possível perceber que a guerra cibernética desafia muita das vezes as normas legais e éticas. A atribuição de ataques cibernéticos é notoriamente difícil, tornando a aplicação das leis internacionais e a identificação de responsabilidades um desafio. Dessa forma as questões éticas em relação à conduta de ataques cibernéticos também se mantêm em constante evolução.

Além disso, à medida que a guerra cibernética se torna mais proeminente, a dissuasão por meio de capacidades cibernéticas se tornou uma parte integral das estratégias de segurança. A ameaça de ataques cibernéticos pode ser usada para desencorajar ações que poderiam levar a conflitos convencionais em primeiro lugar, contribuindo para a manutenção da paz.

6.1 Considerações Finais

Como elucidado na seção dedicada a discussão sobre o estudo de caso, os ataques cibernéticos não se limitam a atos ofensivos. A defesa cibernética é igualmente vital, uma vez que sistemas de segurança robustos são necessários para proteger ativos militares e infraestrutura crítica de ataques cibernéticos inimigos. A falta de segurança cibernética pode deixar as forças expostas a ameaças, comprometendo operações convencionais.

Em resumo, a correlação entre guerra cibernética e guerra tradicional é inegável e complexa. À medida que as fronteiras entre o mundo digital e físico continuam a se fundir, os governos e militares em todo o mundo precisam se adaptar e entender como essa nova dimensão do conflito se encaixa em suas estratégias de segurança. Navegar nesse cenário de conflito híbrido é fundamental para garantir a segurança e a estabilidade internacionais. A guerra cibernética é uma realidade moderna que deve ser enfrentada com responsabilidade, ética e conformidade com as leis internacionais.

6.2 Sugestões para futuros trabalhos

A correlação entre a visão política estratégica e os conhecimentos tecnológicos desempenha um papel crucial nas operações militares contemporâneas, por isso a importância do contato ainda mais cedo do jovem oficial com esse tipo de conceito. Tal importância se evidencia pelos constantes incentivos por parte do Alto Comando da Força em programas como o “Proleitura” e atualmente pela fomentação da busca pelo conhecimento das relações internacionais através de programas informativos como o “ Conexão Geo”.

Dessa forma sugere-se que, em futuras edições do C-Ap-A, sejam considerados a inclusão na lista de temas títulos que possam correlacionar esses dois universos.

REFERÊNCIAS

ALCAIDE, Juan *et al*. Critical infrastructures cybersecurity and the maritime sector. **ScienceDirect**, [*s. l.*], 24 set. 2019.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. 2012. Disponível em: https://www.defesa.gov.br/arquivos/centrais/2012_04_17_publicacao_estrategia_nacional_defesa.pdf. Acesso em: 10 de setembro de 2023.

CAIAFA, R. **Classe Tamandaré – Marinha confirma contrato com empresas.** Disponível em: <https://tecnodefesa.com.br/corvetas-tamandare-marinha-do-brasil-confirma-contratocom-tkms-embraer-atech-e-engeprom/>. Acesso em: 17 out. 2023.

CASE, Andrew *et al*. Hooktracer: Automatic Detection and Analysis of Keystroke Loggers Using Memory Forensics. **ELSEVIER**, [*s. l.*], 19 maio 2020. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0167404820301450. Acesso em: 7 out. 2023.

CASTELLS, Manuel**. A sociedade em rede: A era da informação: economia, sociedade e cultura**. 8 ed. São Paulo: Paz e Terra, 2005.

DE SÁ, A. O.; CARMO, L. F. R. D. C.; MACHADO, R. C. S. Covert Attacks in Cyber-Physical Control Systems. **IEEE Transactions on Industrial Informatics**, v. 13, n. 4, 2017.

Department of Defense, **Quadrennial Defense Review Report** (Washington D.C.: U.S. Department of Defense, 2010).

ESPINOSA, Ágeles. Irã acusa Israel de sabotar sua principal usina nuclear. **El País**, [*S. l.*], p. 1, 12 abr. 2021. Disponível em: https://brasil.elpais.com/internacional/2021-04-12/ira-acusa-israel-de-sabotar-sua-principal-usina-nuclear.html. Acesso em: 19 out. 2023.

FALLIERE, Nicolas; MURCHU, Liam O.; CHIEN, Eric. W32. **stuxnet dossier. White paper**, symantec corp., security response, v. 5, n. 6, p. 29, 2011.

FAOU, Matthieu. TURLA LIGHTNEURON: One email away from remote code execution. **ESET Research White papers**, [*s. l.*], 15 maio 2019. Disponível em: https://web-assets.esetstatic.com/wls/2019/05/ESET-LightNeuron.pdf. Acesso em: 6 out. 2023.

FERNANDES, Cláudio. **Uso de gases tóxicos na primeira guerra mundial**; *Brasil Escola, 2013.* Disponível em Acessado em 5 de outubro de 2023.
FREIRE, Warlley *et al*. Stealth Cyberattack on MIMO Naval Propulsion Systems. **IEEE Computer Society**, [*s. l.*], 1 jun. 2023.
GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 4a ed. São Paulo: Atlas, 2002.

Hjortdal, Magnus. **"China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence."** *Journal of Strategic Security* 4, no. 2 (2011) : 1-24. DOI: http://dx.doi.org/10.5038/1944-0472.4.2.1nAvailable at: https://digitalcommons.usf.edu/jss/vol4/iss2/2

International Institute for Strategic Studies (**IISS**), "The Military Balance 2010, Press Statement," remarks by Dr. John Chipman (February 3, 2010), disponível em: http://tinyurl.com/6abm5pn (www.iiss.org/publications/military-balance/themilitary-balance-2010/military-balance-2010-press-statement/).

KRISCHER, Thais Cristine. **Um estudo da máquina Enigma**. Porto Alegre: UFRGS, 2012. Disponível em: https://www.lume.ufrgs.br/bitstream/handle/10183/66106/000870987.pdf. Acesso em 11 jun. 2019.

LEWIS, Clive. **A abolição do homem**: Um pensamento ardeu na minha mente: por mais que ele dissesse e por mais que me lisonjeasse, vender-me-ia como escravo quando me tivesse em seu poder Bunya. [*S. l.*]: Thomas Nelson Brasil, 1943.

MUELLER, Paul; YADEGARI, Babak. **The Stuxnet Worm**. 2012. Disponível em: http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf. Acessado em abril de 2013.

NATIONAL CYBER SECURITY CENTRE. **Network Defenders, November 2017**. [*S. l.*], 23 set. 2017. Disponível em: https://www.ncsc.gov.uk/static-assets/documents/Turla%20group%20using%20Neuron%20and%20Nautilus%20tools%20alongside%20Snake%20malware_1.pdf. Acesso em: 7 out. 2023.

REYNOL, Fábio. **A corrida tecnológica - como a Guerra Fria impulsionou a ciência.** *Com Ciência, 2012.* Disponível em: http://www.comciencia.br/reportagens/guerra/guerra07.htm. Acessado em: 6 de outubro de 2023.
SÁ, A. O.; MACHADO, R. C. S.; ALMEIDA, N. N. O Encontro da Guerra Cibernética comas Guerras Eletrônica e Cinética no Âmbito do Poder Marítimo. **Revista da Escola deGuerra Naval**, Rio de Janeiro, v. 25, n. 1, p. 89-128. Janeiro/abril. 2019.

Takeuchi, A., Hiroshi, Y., Yamaguchi, K. et al. **Dynamic Link Library for Statistical Analysis and Its Excel Interface**. Computational Statistics 17, 439–452 (2002). https://doi.org/10.1007/s001800200118

GLOSSÁRIO

Air Gap: Isolamento físico ou lógico usado para proteger sistemas de computadores ou redes de acesso não autorizado, especialmente contra ataques cibernéticos.

APT: Termo usado em cibersegurança para descrever ataques cibernéticos altamente direcionados e persistentes. Essas ameaças são conduzidas por atacantes sofisticados, como governos ou grupos cibercriminosos, que têm recursos significativos e objetivos específicos.

MI5: Agência de inteligência doméstica do Reino Unido.

E-mails de *phishing*: Técnica de engenharia social usada por cibercriminosos para enganar e induzir pessoas a revelarem informações confidenciais.

Exploits: Programa ou código de software que aproveita uma vulnerabilidade em um sistema.

SCR: Extensão de arquivo geralmente é associada a arquivos de código-fonte.

Watering Hole: Tipo de ataque cibernético direcionado que visa infectar os visitantes de um site específico.

Rootkit*: Malware* projetado para se esconder profundamente no sistema operacional de um computador ou dispositivo, frequentemente com privilégios de administrador.

Exports**:** Capacidade de um sistema, aplicativo, módulo ou biblioteca de disponibilizar funções, variáveis ou recursos para uso por outros programas ou componentes.

Dropper: Parte de um software malicioso que tem a função de baixar e instalar outros componentes ou partes de um malware em um sistema de computador ou dispositivo.

Wrapper: *Software* ou componente que envolve ou envolve outro programa, biblioteca, serviço ou recurso, geralmente com o objetivo de fornecer uma interface mais amigável, facilitar a integração.

Stub: Comumente usados em programação, teste de software e integração de sistemas para várias finalidades.

***Siemens SIMATIC Step* 7**: *Softwares* de programação de automação industrial mais utilizados no mundo.

Peer-to-peer: Modelo de rede de computadores em que os dispositivos, como computadores, servidores, ou outros dispositivos, se comunicam diretamente entre si, sem a necessidade de um servidor centralizado.

OSINT: Processo de coleta, análise e interpretação de informações obtidas a partir de fontes de acesso público.

Overshoots: Extensão pela qual uma resposta excede o valor de pico desejado em uma resposta transitória a uma mudança de entrada. É um fenômeno indesejado que ocorre em sistemas de controle quando o sistema responde exageradamente a uma mudança no sinal de entrada antes de se estabilizar.

***Honeypot* PLC**: Forma específica de honeypot que é projetada para atrair e detectar ataques direcionados a Controladores Lógicos Programáveis (PLCs).

***Firewall* Industrial**: Componente de segurança de rede ou software projetado para proteger uma rede de computadores ou dispositivo individual contra ameaças cibernéticas, como ataques, *malware* e acesso não autorizado.