ESCOLA DE GUERRA NAVAL

CC (T) Roberta Rodriguez Corrêa

DEFESA CIBERNÉTICA:
O EMPREGO DE PLATAFORMA DE INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS PELA MB NO ENFRENTAMENTO DA EVOLUÇÃO DAS AMEAÇAS

Rio de Janeiro

2022

CC (T) Roberta Rodriguez Corrêa

DEFESA CIBERNÉTICA:
O EMPREGO DE PLATAFORMA DE INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS PELA MB NO ENFRENTAMENTO DA EVOLUÇÃO DAS AMEAÇAS

Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso Superior.

Orientador: CF (FN) Salvador Mota Junior.

Rio de Janeiro

Escola de Guerra Naval

2022

RESUMO

A adoção do trabalho remoto como herança da pandemia COVID-19 e a dependência cada vez maior das redes e sistemas conectados à Internet possibilitaram o aumento da superfície de ataques cibernéticos disparados por ameaças com diferentes interesses. O Brasil, preocupado com o aumento crescente de ataques cibernéticos, apresentou, por meio da Política Nacional de Defesa, o setor cibernético como estratégico para o país, incumbindo à Marinha do Brasil tarefas que contribuem para a defesa cibernética nacional. Diante da rápida evolução das ameaças, visando a objetivos escusos, e a pouca eficiência de ferramentas tradicionais de segurança em combater ataques com alto grau de sofisticação, diversas organizações têm recorrido ao emprego da Inteligência de Ameaças Cibernéticas. Apesar de a Marinha do Brasil empreender atividades e investimentos neste campo, percebeu-se as necessidades de automatização de parte desse processo, diante do grande volume de informações de alertas oriundos de ferramentas tecnológicas, e a de comunicação e tomada de decisão mais ágil. Face a essa questão, buscou-se demonstrar quais contribuições o emprego de uma Plataforma de Inteligência de Ameaças Cibernéticas poderia trazer à Força naval para combater ameaças de forma eficaz. Para tanto, foi traçado um histórico evolutivo das ameaças e suas capacidades, bem como a descrição das Plataformas de Inteligência de Ameaças Cibernéticas por características e funcionalidades. Além disso, analisaram-se possibilidades do emprego de uma Plataforma pela MB, a fim de maximizar os benefícios de implantação de um programa de inteligência único para o enfrentamento de ameaças.

Palavras-Chave: Evolução de Ameaças. Defesa Cibernética. Inteligência de Ameaças Cibernéticas. Plataforma de Inteligência de Ameaças Cibernéticas.

LISTA DE ABREVIATURAS E SIGLAS

APT — *Advanced Persistent Threat*

CIM — Centro de Inteligência da Marinha

CRITS — *Collaborative Research Into Threats*

CIF — *Collective Intelligence Framework*

CoNavOpEsp — Comando Naval de Operações Especiais

ComDCiber — Comando de Defesa Cibernética

DLP — *Data Loss Prevention*

DCTIM — Diretoria de Comunicações e Tecnologia da Informação da Marinha

DoS — *Denial of Service*

DDoS — *Distributed Denial of Service*

DGMM — Diretoria-Geral do Material da Marinha

Eciber — Espaço Cibernético

EMCFA — Estado-Maior Conjunto das Forças Armadas

END — Estratégia Nacional de Defesa

GE — *General Eletric*

GptOpGCiber — Grupamento Operativo de Guerra Cibernética

IOC — *Indicator of Compromise*

IDS — *Instrusion Deteccion System*

IPS — I*ntrusion Prevention System*

MISP — *Malware Information Sharing Platform*

MB — Marinha do Brasil

NSA — *National Security Agency*

OSINT — *Open Source Intelligence*

PND — Política Nacional de Defesa

SMDC — Sistema Militar de Defesa Cibernética

SCADA — *Supervisory Control and Data Acquision*

SIEM — *Security Information and Event Management*

SIC — Segurança da Informação e Comunicações

TIP — *Threat Intelligence Platform*

SUMÁRIO

1 INTRODUÇÃO.....6

2 EVOLUÇÃO DAS AMEAÇAS.....9

2.1 Ameaças Cibernéticas.....9

2.2 Breve histórico: da década de 70 à atualidade.....11

2.3 Tipos de ataques cibernéticos.....13

2.4 Transversalidade.....15

3 PLATAFORMAS DE INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS.....17

3.1 Inteligência.....17

3.2 Inteligência de Ameaças Cibernéticas.....19

3.2.1 Fontes de Inteligência de Ameaças Cibernéticas.....20

3.3 Plataformas de Inteligência de Ameaças Cibernéticas.....21

4 PLATAFORMA DE INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS NA MB.....24

4.1 A Defesa Cibernética no Brasil.....25

4.2 A Defesa Cibernética na MB.....26

4.2.1 A Inteligência de Ameaças Cibernéticas na MB.....28

4.2.2 Emprego da Plataforma de Inteligência de Ameaças Cibernéticas na MB.....30

5 CONCLUSÃO.....32

REFERÊNCIAS.....35

1 INTRODUÇÃO

A pandemia da COVID-19 transformou as relações de trabalho e estabeleceu o *home-office* como uma prática eficiente e menos custosa que a presencial. Com isso, houve um aumento do uso de ferramentas *on-line* para acesso remoto às redes corporativas privadas e governamentais o que despertou a atenção de criminosos devido à possibilidade de expansão significativa da superfície de ataque no Espaço Cibernético (ECiber), aliada à evolução qualitativa das ameaças na exploração de vulnerabilidades de sistemas e redes.

No Cenário Internacional, é cada vez mais frequente o uso do ECiber como campo de embate político e projeção de poder e influência sobre os Estados-Nações. Em 2016, por exemplo, os EUA responsabilizaram a Rússia por um ataque cibernético que violou e-mails do Partido Democrata numa tentativa de influenciar as eleições norte-americanas (VEJA, 2016). Mais recentemente, em 2020, autoridades norte-americanas atribuíram ao serviço de espionagem russo a autoria de um ataque cibernético em grande escala à fabricante de software *SolarWinds*, afetando organizações privadas e departamentos governamentais (FOLHA, 2021).

Nas últimas décadas, as tradicionais ameaças, tais como: terroristas, Estados e criminosos evoluíram ao explorar o domínio cibernético das mais diversas formas: prática de crimes, espionagem e política. Estados, por exemplo, passaram a evitar o embate direto em conflitos, reduzindo os gastos com armamento e o risco de perda humana, ao lançar ataques cibernéticos direcionados às infraestruturas críticas (sistema financeiro, sistema de fornecimento de água, energia, serviços de saúde, transporte e indústria).

Para consecução desses objetivos, utilizam-se de ataques cada vez mais elaborados e de difícil detecção, como as APT (sigla em inglês para ameaças persistentes avançadas) que visam coletar informações pessoais ou de inteligência nacional. Ameaças desse tipo em muito se diferem das ameaças do início dos anos 2000 com ações rudimentares e típicas de *hacktivistas*[1].

Considerando esse cenário, o Brasil, por entender que a segurança e a defesa do espaço cibernético brasileiro requerem especial atenção, haja vista serem essenciais para

1 Ativistas hackers que realizam ataques cibernéticos com o fim de promover uma ideologia política (elaborado pela autora).

garantir o funcionamento dos sistemas de informações, de gerenciamento e de comunicações de interesse nacional (BRASIL, 2012), por meio da sua Estratégia Nacional de Defesa (END), apresentou o setor cibernético como estratégico para a Política Nacional de Defesa (PND), a qual atribuiu como tarefa para as Forças Singulares, que são componentes da Estrutura Cibernética de Defesa, a colaboração com as atividades de Inteligência de fonte cibernética em proveito das atividades do Sistema Militar de Defesa Cibernética (SMDC).

No âmbito da MB, o Centro de Inteligência da Marinha (CIM), Organização Militar (OM) responsável pelo tratamento do assunto no âmbito da Força Naval, tem realizado as tarefas de Inteligência Cibernética e apoio às Ações de Guerra Cibernética, que envolvem a Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) e o Comando Naval de Operações Especiais (CoNavOpEsp) (BRASIL, 2021). Apesar disso, faz-se necessário que a MB adote mecanismos cada vez mais aperfeiçoados que permitam um panorama de consciência situacional cibernético que traduza a realidade frente à ameaças mais resilientes e menos detectáveis. Acredita-se que um dos mecanismos viáveis seria a aquisição de tecnologia que automatize a integração e processamento de um grande volume de informações obtidas de ferramentas de gerenciamento e segurança de redes de computadores, que seja capaz de filtrar ameaças relevantes.

Nesse sentido, a adoção de Plataforma de Inteligência de Ameaças Cibernéticas tem auxiliado organizações na antecipação e prevenção de ameaças cibernéticas, além de permitir o aprimoramento crescente dos mecanismos de Defesa Cibernética de acordo com o contexto organizacional.

Diante desse quadro, buscou-se, com este trabalho científico, demonstrar possíveis contribuições do uso de Plataforma de Inteligência de Ameaças, caso fosse implantada pela MB, na sua tarefa de prevenção e mitigação de ataques cibernéticos. Em suma, a questão é: de que forma o uso de Plataforma de Inteligência de Ameaças Cibernéticas pode contribuir na prevenção e mitigação de ataques cibernéticos, uma vez que a Marinha, na sua tarefa de proteger o ECiber-MB, deve empregar soluções que promovam uma análise rápida e eficaz na detecção e compreensão das ameaças para combatê-las? Para esse fim, estabeleceu-se três objetivos específicos. No primeiro, buscou-se descrever como as ameaças evoluíram ao longo das décadas. No seguinte, procurou-se descrever os propósitos, características e funcionamento das Plataformas de Inteligência de Ameaças

Cibernéticas. Por último, foi realizada uma análise das contribuições na utilização de uma Plataforma de Inteligência de Ameaças Cibernéticas.

Desse modo, com base nos elementos citados anteriormente e nas informações coletadas sobre como a MB realiza a Inteligência de Ameaças Cibernéticas, o presente trabalho busca apresentar possíveis contribuições do uso de Plataforma de Inteligência de Ameaças Cibernéticas pela Estrutura de Defesa Cibernética da MB em resposta ao problema de pesquisa.

A presente pesquisa é motivada por três razões. A primeira, por interesse pessoal aos assuntos relacionados a Defesa Cibernética. A segunda, pelo uso cada vez mais frequente de ataques cibernéticos por Estados-Nações em conflitos para atingir objetivos militares. Por fim, pela condição de um Oficial da Marinha que tem entre as suas atribuições contribuir com soluções que promovam o aperfeiçoamento dos processos e ferramentas utilizados pela instituição.

Este estudo constitui-se de uma pesquisa bibliográfica realizada em literaturas técnicas, trabalhos acadêmicos, sítios de órgãos e instituições públicas e privadas, estudos de formulações de proposições de normas técnicas em andamento na MB e de normas técnicas internacionais. Após a leitura e fichamento do material coletado, todo conteúdo foi interpretado visando alcançar o objetivo geral do trabalho.

O assunto em tela mostra-se relevante, na medida em que houve um aumento no número de ataques cibernéticos no Brasil nos últimos dois anos, sendo necessário envidar esforços no conhecimento das ameaças e na realização de medidas que promovam o fortalecimento da Defesa Cibernética na MB. É relevante ainda, diante da repercussão que o assunto tem tomado, principalmente no cenário internacional, nos conflitos envolvendo grandes potências como a Rússia, EUA e China.

Estrutura-se este trabalho em três seções. Na primeira, tratar-se-á, de uma forma geral, a respeito da evolução das ameaças, tipos de ataques cibernéticos utilizados por essas ameaças e a transversalidade desses ataques. Na segunda seção, serão apresentados os principais conceitos de Inteligência de Ameaças Cibernéticas e o funcionamento de Plataformas de Inteligência de Ameaças Cibernéticas com foco naquelas de código aberto. Por fim, na última seção será realizada uma análise, com base nos dados coletados nas seções anteriores e dos documentos da Marinha, visando a identificar

possíveis respostas ao objeto deste trabalho. Espera-se que a presente pesquisa possa contribuir com estudos acadêmicos sobre o tema, principalmente com os dados que serão apresentados, de forma a favorecer outros pesquisadores interessados em dar-lhe continuidade, tornando viável uma implantação de uma solução desse tipo na Marinha do Brasil (MB).

2 EVOLUÇÃO DAS AMEAÇAS

Nesta seção pretende-se identificar as ameaças cibernéticas e apresentar um breve histórico dos acontecimentos a fim de compreender como essas ameaças se originaram e como elas evoluíram ao logo tempo e suas motivações. Após o histórico, serão citados os principais ataques cibernéticos utilizados e como eles são empregados no contexto de Guerra Cibernética, impactando nas instituições privadas e governamentais.

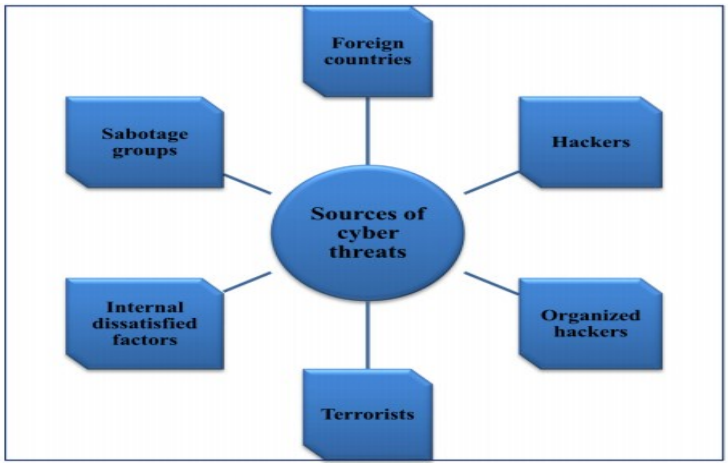
2.1 Ameaças Cibernéticas

Ao longo dos anos, a Internet vem desempenhando um importante papel na comunicação e integração de bilhões de usuários devido ao seu baixo custo e a possibilidade de acesso a sistemas das mais diversas áreas, tais como: saúde; comércio; banco; cultura; educação; economia e governo, mesmo que esses sistemas se encontrem de maneira dispersas pelo globo — em países ou até mesmo em continentes diferentes, pois, uma vez que o usuário esteja conectado ao espaço cibernético, o acesso independe da localização geográfica.

A dependência dos usuários por produtos globalizados de *hardwares* e *softwares* para comunicação acende um alerta para as questões de segurança com relação à confiabilidade do processo da cadeia de suprimento desses produtos sujeitos à manipulação de ameaças cibernéticas (LI; LIU, 2021).

Consideram-se fontes de ameaças cibernéticas os seguintes atores: governos, grupos de crime organizado, ativistas, terroristas e espiões. Elas se diferenciam das tradicionais ameaças, cujos atores, normalmente governos e nações, costumam ser mais facilmente identificáveis numa área geográfica (LI; LIU, 2021). A figura 1 ilustra a diversidade de ameaças que permeiam o espaço cibernético com diferentes interesses.

Figura 1 - ameaças do espaço cibernético



Fonte: LI; LIU (2022, p.5).

Segundo Brasil (2014, p. 18), o espaço cibernético é definido como o "espaço virtual, composto por dispositivos computacionais conectados em redes ou não, em que as informações digitais transitam, são processadas e/ou armazenadas". Devido à natureza globalizada da Internet e a ausência de fronteiras do ECiber, esses grupos passaram a explorar este espaço como um novo campo de batalha, emergindo no mundo virtual e vislumbrando uma nova forma de conflito capaz de produzir amplos efeitos no mundo real (LI; LIU, 2021) e de se distanciar do embate direto (PINTO; GRASSI, 2021).

Estados-Nações podem optar por uma Guerra Cibernética, obtendo vantagens táticas ou estratégicas ao impor danos físicos diretos ao inimigo ou manipulando informações táticas num Teatro de Operações (CLARK; KNAKE, 2010; ZETTER, 2014). Serviços de Inteligência de países estrangeiros podem utilizar ferramentas voltadas para espionagem e coleta de informações visando ao ataque às infraestruturas críticas de outro país. Ativistas hackers, conhecidos como *hacktivistas*, motivados politicamente, seriam capazes de desfigurar sítios eletrônicos corporativos para publicar mensagens de protestos. Uma outra importante ameaça externa, são os terroristas que desferem ataques às infraestruturas vitais para enfraquecer a segurança nacional e a confiabilidade da sociedade perante seu Estado.

As preocupações com as ameaças devem ser estendidas também ao âmbito interno organizacional. Funcionários insatisfeitos podem vazar informações ou ainda atacar sistemas aproveitando-se do seu conhecimento sobre a instituição em que trabalha e dos

acessos que possui às redes e sistemas (LI; LIU, 2021).

2.2 Breve histórico: da década de 70 à atualidade

Antes mesmo da difusão da Internet, nos anos 70, soviéticos desenvolveram um programa de espionagem denominado Line X com o intuito de furtar *software* dos países ocidentais. Em 1981, os Estados Unidos descobriram o programa espião e, numa ação ofensiva, inseriram uma bomba lógica[2] no *software* canadense de controle de gasodutos adquirido pelos soviéticos. O *malware* ficou adormecido por um tempo para não ser detectado e, quando tornou-se ativo, fez com que as válvulas do gasoduto Transiberiano começassem a abrir e fechar, fazendo com que pressão interna das bombas aumentassem, levando, segundo os EUA, a uma explosão em junho de 1982. A mídia russa nega que a explosão tenha ocorrido (SUPER INTERESSANTE, 2016).

A década de 80 é marcada por discussões em torno da segurança cibernética, devido à expansão da rede de telecomunicação e de computadores pessoais e do crescimento dos chamados "vírus de computador". Países como os EUA passaram a se preocupar com a possibilidade de espionagem de segredos militares e industriais por outros países (AVELAR, 2018) e grandes empresas viram no mercado uma oportunidade de alavancar as vendas com antivírus (CISOMAG, 2021).

Na década de 90, os primeiros guerreiros cibernéticos americanos começaram a estudar meios de derrubar a rede de radares e mísseis da defesa antiaérea iraquiana antes de avançar em direção a Bagdá (CLARK; KNAKE, 2010). Na mesma época, as redes da empresa *General Eletric* (GE) e da TV americana NBC foram invadidas, causando prejuízos na ordem de milhões de dólares (AVELAR, 2018). De igual impacto, em 1994, hackers russos e americanos invadiram os computadores do *Citibank* em Nova York e roubaram cerca de 10 milhões de dólares (SUPER INTERESSANTE, 2016).

Em 2007, a Estônia foi alvo de um ataque de negação de serviço distribuído (DDoS), o maior visto até aquele momento, direcionado aos sítios de Internet (SHEETER, 2007), de servidores da rede telefônica, do sistema de cartões de créditos e do serviço de diretório da Internet, impactando no funcionamento de bancos, comércio e serviços de

2 Código malicioso inserido em sistema para causar danos em condições estabelecidas pelo atacante (elaborado pela autora).

comunicação de todo o país (CLARK; KNAKE, 2010; ZETTER, 2014). O ataque foi motivado pela decisão do país de transferir, do centro de Tallinn para um cemitério militar, uma estátua que comemorava o combate dos nazistas pelos soldados do Exército Vermelho na Segunda Guerra Mundial, gerando uma crise diplomática com a Rússia (KOTTASOVÁ, 2021), principal suspeito dos ataques.

No ano seguinte, a Rússia entrou em conflito com a Geórgia devido às províncias de Ossétia do Sul e Abkházia. Esses territórios, que chegaram a ser de domínio russo, haviam conseguido estabelecer a independência, embora legalmente pertencentes à Geórgia e dependente financeiramente da Rússia. Em julho de 2008, rebeldes de Ossétia do Sul lançaram ataques de mísseis contra aldeias georgianas. Em resposta ao ataque, o exército georgiano bombardeou e ocupou a capital. No dia seguinte à invasão, o exército russo avançou no território no intuito de expulsar o exército georgiano ao mesmo tempo em que guerreiros cibernéticos russos desferiram ataques DDoS aos meios de comunicação e sítios do Governo. Rebeldes de Abzkházia aproveitaram a situação e expulsaram os georgianos com o auxílio de aliados russos (CLARK; KNAKE, 2010; ZETTER, 2014).

Em 2010, o *worm* Stuxnet, tinha como alvo as centrífugas de enriquecimento de urânio. Suspeita-se que os EUA e Israel estejam por trás do artefato que alterava os parâmetros do sistema SCADA[3], fazendo com que as centrífugas se danificassem ao operar fora das condições normais. Isso provocou um atraso de dois anos no programa nuclear iraniano (SHAKARIAN, 2011). O sistema SCADA pode ser encontrado em outros equipamentos industriais, como os que compõem usinas hidrelétricas e embarcações.

Em 2013, o ex-técnico da CIA Edward Snowden procurou a imprensa para revelar sobre os programas de vigilância que os EUA utilizam para espionar a população norte-americana, países da América Latina e Europa. Em uma das revelações, citou o monitoramento dos e-mails da ex-presidente Dilma Roussef e de seus assessores. Após uma semana da referida citação, publicou documentos da *National Security Agency* (NSA) com indícios que demonstram o interesse dos norte-americanos na tecnologia de exploração em alta profundidade na camada pré-sal, utilizada pela Petrobrás. (BBC, 2013).

No Brasil, em dezembro de 2021, as plataformas ConecteSUS, e-SUS Notifica e SI-PNI ficaram indisponíveis aos usuários por treze dias após um ataque cibernético

3 Sistema que realiza o controle de equipamentos da indústria em tempo real (elaborado pela autora).

direcionado ao Ministério da Saúde. Com isso, serviços como a emissão do Certificado Nacional de Vacinação e o agendamento de vacinação não puderam ser acessados (CNN, 2022).

Mais recentemente, no ano 2022, vemos no conflito entre a Rússia e a Ucrânia uma guerra híbrida, em que, além da Guerra Cinética, com o emprego de tanques e mísseis, há também a Guerra Cibernética. Esses conceitos são bem definidos a seguir:

> Guerra Cibernética é o sub-conjunto da guerra da informação que envolve ações realizadas no mundo cibernético. O mundo cibernético é qualquer realidade virtual compreendida numa coleção de computadores e redes. Existem diversos mundos cibernéticos, mas o mais relevante para a Guerra Cibernética é a Internet e as redes a ela relacionadas, as quais compartilham mídia com a Internet. A definição militar mais próxima para o nosso termo, guerra cibernética, é uma combinação de ataque a redes de computadores e defesa de redes de computadores, e possivelmente, operações especiais de informação. Nós definimos guerra cinética como sendo a guerra praticada no "mundo real". Todos os tanques e navios e aviões e soldados tradicionais são os protagonistas da guerra cinética (tradução do autor) (PARKS, DUGGAN, 2001, p. 30 *apud* DUTRA, 2007, p. 1).

Se compararmos os ataques russos de 2015 e 2016 que resultaram no apagão da rede elétrica da Ucrânia e o ataque russo com *ransomware* que bloqueou as operações do oleoduto norte-americano, podemos considerar que a Rússia, uma potência no campo cibernético, pouco tem atacado à Ucrânia. A maioria dos ataques do atual conflito tem sido direcionado a sítios do governo e ao sistema bancário ucraniano (TIDY, 2022).

Percebe-se ao longo das décadas que os artefatos utilizados pelas ameaças cibernéticas em seus ataques estão cada vez mais sofisticados na medida em que o mundo avança tecnologicamente. A seguir serão definidos os tipos de ataques cibernéticos mais comuns.

2.3 Tipos de ataques cibernéticos

À medida que novos e diferentes dispositivos são interconectados na Internet, aumenta a superfície e as possibilidades de ataque a ser explorada pelas ameaças cibernéticas, crescendo as invasões em número e sofisticação. Dentre os tipos de ataque mais comuns, destacam-se: DoS (*Denial of Service*), DDoS (*Distributed Denial of Service*), bomba lógica, cavalo de tróia, vírus e *worm* (LI; LIU, 2021).

Os ataques de negação de serviço, chamados de DoS, sobrecarregam um

servidor com grande quantidade de pacotes de dados para tornar indisponível os recursos aos seus utilizadores. Esses ataques podem ainda assumir uma configuração distribuída, denominada DDoS, negação de serviço distribuída. Nos ataques de DDoS, o atacante invade um computador mestre e por meio dele controla várias outras máquinas denominadas zumbis, normalmente por meio da multiplicação de *worm*, enviando simultaneamente vários pedidos de acesso ao servidor até torná-lo indisponível. Tanto o DoS quanto o DDoS são bastante utilizados para prática de extorsão em que o invasor cobra um resgate para colocar o serviço disponível sem qualquer garantia (COSTA, 2014).

Num ataque de bomba lógica, um código é inserido num programa com o objetivo de realizar determinada atividade destrutiva em condições e data específica.

Já os vírus são anexados a documentos ou arquivos executáveis e necessitam da interação humana para se espalharem, como o download de anexo de e-mail ou compartilhamento de arquivos.

Diferente dos vírus, os *worms* são programas autônomos que, ao entrar no sistema, via conexão rede ou arquivo baixado, criam cópias de si para propagá-las pela rede no intuito de contaminar estações de trabalho vulneráveis (KASPERSKY, 2022).

Um outro programa, aparentemente inofensivo, que ao ser utilizado executa atividades maliciosas, é o cavalo de tróia. Um exemplo de cavalo de troia bastante atual é o *infostealer*, encontrado em programas “crackeados”, que rouba informações bancárias, *login*, fotos e documentos com o objetivo de recompensar financeiramente criminosos (BARBOSA, 2022). Para 2022, especialistas em segurança da informação alertam para outros dois ataques: *deepfake* e *ransomware*.

O d*eepfake* usa técnicas de *phishing* e inteligência artificial para imitar imagem e voz de pessoas com o objetivo de convencer funcionários de empresa que trabalham remotamente a fornecer informações confidenciais.

Já o *ransomware* impossibilita o acesso a arquivos através de criptografia. Para reaver o acesso, é cobrado um resgate em criptomoedas pelo criminoso, o que nem sempre é garantido (BARBOSA, 2022).

Apesar dos esforços das organizações em se protegerem desses ataques por meio da implementação das tradicionais ferramentas de segurança, segundo Tousin e Rais (2018) *apud* Azevedo (2020), elas não são eficientes para a nova geração de ameaças

cibernéticas, caracterizadas por serem evasivas, resilientes e persistentes. As ameaças cibernéticas citadas por Tousin e Rais (2018) dizem respeito aos ataques cibernéticos e não aos atores apresentados anteriormente.

Essas ameaças costumam ter alvos e objetivos específicos que, para alcançá-los, utilizam-se de técnicas que garantam a persistência no alvo de forma transparente, como as *Advanced Persistent Threats* (APTs).

A APT é uma tipo de ataque cibernético que possibilita a permanência indetectável por um longo período no alvo, devido ao uso de *malwares* que têm como característica o polimorfismo, ou seja, a capacidade constante de modificação (SILVA, 2020).

As ameaças polimórficas utilizam-se de vírus, *worm* ou cavalo de troia com capacidade constante de mutação do código que pode resultar na alteração do nome ou compactação do arquivo. Essa mutação tem por objetivo evitar sua detecção, no entanto sua funcionalidade continua a mesma.

Outras duas ameaças desta nova geração são os *Zero-Day* e os ataques compostos (AZEVEDO, 2020). Num ataque *Zero-Day*, ameaças exploram vulnerabilidades de *software* não conhecidas pelo fabricante, tampouco pelos seus usuários. Esse desconhecimento permite que ameaças explorem as brechas com o auxílio de artefatos cibernéticos até que o fabricante descubra a vulnerabilidade e desenvolva uma correção para saná-la (BRASIL, 2021). Já no ataque composto, são utilizadas técnicas de ataques sintáticos que exploram vulnerabilidades técnicas em *hardware* ou *software* (vírus, *worm* e cavalo de tróia) e ataques semânticos que exploram as fraquezas do comportamento do ser humano, como o *phishing*[4] (AZEVEDO, 2020).

Ameaças sofisticadas, como essas, são mais comumente encontradas num contexto de Guerra Cibernética, devido a sua transversalidade.

2.4 Transversalidade

A Guerra Cibernética é transversal às corporações privadas e governamentais, impacta nos poderes políticos, econômicos, culturais e de ciência e tecnologia, além de refletir nos demais domínios como o eletrônico e o cinético (MOTA; MOTA, 2019).

4 Fraude que se utiliza de técnicas para enganar as pessoas visando a obtenção de informações privilegiadas (elaborado pela autora).

Um dos principais alvos num cenário de Guerra Cibernética são sistemas relacionados às infraestruturas críticas, pois os danos causados dificultam um país de manter sua capacidade de reação e defesa (SILVA, 2014). Diante desse cenário, é imperiosa a necessidade de aprimoramento da Defesa Cibernética das infraestruturas críticas do país (MOTA; MOTA, 2019) para torná-la resiliente e possibilitar um planejamento para seu restabelecimento em caso de uma ataque.

As infraestruturas críticas correspondem aos bens, serviços e instalações cuja interrupção ou destruição pode provocar prejuízos econômicos, políticos, à segurança da sociedade e do Estado (BRASIL, 2010). Programas de computador que gerem ou controlam os setores econômicos ou empresariais bem como os serviços públicos têm sido alvos preferenciais, dentre eles podemos citar: comando das redes de distribuição de energia elétrica, comando das redes de comunicações em geral, comando da rede do Ministério da Defesa e comando das redes de distribuição de água potável (FERNANDES, 2012). No mesmo conceito de infraestrutura crítica, podemos abarcar, por exemplo, o Poder Marítimo, considerando que os sistemas navais estão cada vez mais integrados aos sistemas de comunicação, plantas físicas e sensores do espectro eletromagnético. Ações ofensivas que permeiam os domínios cibernéticos, eletrônico e cinético podem causar impactos nos setores de transporte, energia, defesa e alimentos (SÁ *et al.*, 2019).

Para combater as ameaças inerentes à Guerra Cibernética de forma transversal, dentre elas espiões, terroristas e Estados, as estratégias de defesa devem introduzir mecanismos de inteligência cibernética alinhada com componentes da inteligência, a saber: planejamento e direção, levantamento de dados, processamento, produção e disseminação.

Diante do atual cenário, observamos que a história vem demonstrando o emprego cada vez mais sofisticado dos ataques cibernéticos por grupos organizados às infraestruturas críticas de um Estado para obter vantagens estratégicas. Esses ataques utilizam técnicas avançadas de persistência e são de difícil detecção por soluções tradicionais de segurança. Muitos dos sistemas utilizados por essas infraestruturas são comuns tanto às corporações governamentais quanto empresas privadas, fazendo com que as vulnerabilidades sejam igualmente exploradas e impactando os serviços prestados de forma transversal.

Proteger as infraestruturas de redes e sistemas de ameaças sofisticadas torna-se

um desafio, pois requer das organizações conhecimento estratégico dessas ameaças para adoção de uma postura proativa de defesa (SILVA, 2020).

3 PLATAFORMAS DE INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS

Esta seção visa, inicialmente, trazer os conceitos de Inteligência e Inteligência de Ameaças Cibernéticas que são empregados na produção de conhecimento sobre ameaças cibernéticas em constante evolução. Descreve ainda, as características e funcionalidades das Plataformas de Inteligência de Ameaças Cibernéticas com foco naquelas que são gratuitas.

3.1 Inteligência

O monitoramento humano das ameaças por meio de alertas e eventos mal-intencionados, gerados por ferramentas de segurança, e a resposta direta a incidentes de segurança não têm demonstrado eficiência na detecção de ataques sofisticados como os já citados APT e *Zero-Day*. Primeiramente, devido ao demasiado tempo para análise, filtro e categorização das informações recebidas por essas ferramentas de segurança. Segundo, pela carência de informações em quantidade suficiente para tomada de decisão precisa e construção de mecanismos de defesa adequados ao contexto (SILVA, 2020).

A adequação dos mecanismos de defesa deve ocorrer na mesma proporção em que as ameaças evoluem. Para que isso seja possível, as organizações devem produzir conhecimento estratégico sobre as ameaças existentes ou emergentes que possam trazer danos. A produção desse conhecimento é alcançada pelo emprego de um campo de conhecimento denominado Inteligência de Ameaças Cibernéticas (AZEVEDO, 2020).

Antes de adentrarmos no conceito de Inteligência de Ameaças Cibernéticas, é primordial o entendimento dos conceitos de: dados, informação e conhecimento. O quadro 1 apresenta esses conceitos definidos no âmbito da segurança cibernética.

Quadro 1 - Dado x Informação x Conhecimento

Tipo	**Descrição**	**Segurança Cibernética**
Dado	Consiste em fatos e estatísticas discretas, reunidos como base para uma análise mais aprofundada.	Os dados geralmente são apenas indicadores, como endereços IP ou URL. Os dados não nos dizem muito sem análise.
Informação	São vários pontos ou conjunto de dados combinados para responder a perguntas específicas.	As informações respondem a perguntas como: “Quantas vezes minha organização foi mencionada nas mídias sociais esse mês?”. Embora seja uma saída muito mais útil que os dados brutos, ainda não informa diretamente uma ação específica.
Conhecimento	Analisa dados e informações para descobrir padrões e histórias que orientem a tomada de decisão.	O conhecimento é produto de um ciclo de identificação de perguntas e objetivos, coleta de dados relevantes, processamento e análise desses dados, resultando na produção de inteligência que proporciona ações e compartilhamento.

Fonte: AZEVEDO *apud* AHLBERG (2020, p. 27).

Os dados brutos são agrupados em conjuntos menores de dados relevantes sobre ameaças. Depois esses dados são relacionados, processados e transformados em informação. Essa informação então passa por um processo de análise e contextualização que dá origem ao conhecimento que, quando aplicado, produz a inteligência (AZEVEDO, 2020).

Uma inteligência deve ser completa e precisa o suficiente para permitir uma tomada de decisão, relevante ao abordar questões relacionadas à missão da organização e

oportuna ao ser entregue no tempo correto (KLINCZAK, 2019).

Quando relacionada às ameaças, a Inteligência busca responder quais agentes possuem pretensão de realizar ataques cibernéticos, quais técnicas serão utilizadas e sua capacidade de sucesso (KLINCZAK, 2019). Dentro do espectro da Inteligência de Ameaças está a Inteligência de Ameaças Cibernéticas, descrita na subseção a seguir.

3.2 Inteligência de Ameaças Cibernéticas

A Inteligência de Ameaças Cibernéticas pode ser definida como o conhecimento baseado em evidências, contexto, mecanismos, indicadores (padrões utilizados para detectar atividades suspeitas ou maliciosas) e implicações sobre uma ameaça existente ou emergente que permite, às organizações, ações em resposta a essas ameaças (AZEVEDO, 2020 *apud* MCMILLAN, 2020).

Análises, baseadas em Inteligência de Ameaças Cibernéticas, favorecem a implementação de medidas de defesa mais resilientes aos ataques. Ao priorizar os investimentos em tecnologia e contramedidas essenciais no contexto organizacional, o esforço empreendido pela ameaça para alcançar seus objetivos aumenta (AZEVEDO, 2020). A execução dessas ações deve ocorrer na velocidade da evolução dessas ameaças.

Para que a Inteligência de Ameaças Cibernéticas traga resultados satisfatórios, é preciso inicialmente definir os requisitos da organização com relação a sua obtenção e o contexto no qual está inserida. Definidos os requisitos, os dados são coletados, processados, transformados e analisados para que a informação seja estruturada e os padrões sejam identificados. Essas informações transformadas podem ser integradas a outros mecanismos de defesa e usadas na implementação de medidas que visam mitigar as ameaças (SILVA, 2020 *apud* FRIEDMAN, 2020).

O entendimento do cenário de ameaças cibernéticas pode ser ainda potencializado com o compartilhamento e disseminação dessas informações entre organizações (SILVA, 2020 *apud* BARNUM, 2020). Na prática, esse compartilhamento proporciona um incremento no conhecimento de ameaças emergentes, reduz as lacunas de habilidades entre as equipes de Defesa Cibernética e permite a troca de experiência operacional entre os participantes, aprimorando a defesa das redes e sistemas contra ataques cibernéticos contínuos (AZEVEDO, 2020).

A Inteligência de Ameaças Cibernética atua nos três níveis organizacionais: tático, operacional e estratégico.

No nível estratégico, fornece uma visão de alto nível da evolução das ameaças, auxiliando a Administração na tomada de decisão. Fontes de Inteligência de Ameaças Cibernéticas no nível estratégico incluem tendências históricas, assuntos geopolíticos e dados contextuais, uma vez que ameaças passadas geralmente influenciam ataques futuros (FLASHPOINT, 2022; UNITED KINGDOM (UK), 2019).

De natureza acionável, a Inteligência de Ameaças Cibernéticas no nível operacional foca nos possíveis ataques que a organização está sujeita em tempo real, oferecendo informações sobre as motivações, infraestrutura, capacidade e alvos. Isso permite que gerentes de segurança da informação aloquem recursos para ações defensivas contra ameaças consideradas de alta prioridade. Fontes de inteligência de ameaças de nível operacional incluem relatórios de agentes de ameaças, relatórios de incidentes, análise de *malware* e, ocasionalmente, mídias sociais e salas de bate-papo (FLASHPOINT, 2022; UK, 2019).

Já no nível tático, preocupa-se com informações sobre Táticas, Técnicas e Procedimentos (TTP) e Indicadores de comprometimento (IOCs) de atacantes. Indicadores de comprometimento são evidências que indicam que a segurança de uma rede ou sistema foi comprometida, como por exemplo, uma atividade de acesso a sítios maliciosos. As TTP e os IOCs são necessários para a construção de um plano de defesa. Além disso, a Inteligência de Ameaças Cibernéticas de nível tático contextualiza eventos isolados, auxiliando a defesa na priorização e classificação de urgência das diversas ameaças. Suas fontes mais comuns incluem relatórios de incidentes e *logs* de auditoria e monitoramento (FLASHPOINT, 2022; UK, 2019).

3.2.1 Fontes de Inteligência de Ameaças Cibernéticas

As fontes de Inteligência de Ameaças Cibernéticas podem ser oriundas de dentro da organização (interna) ou fora dela (externa).

Fontes internas dizem respeito aos dados que são monitorados e coletados dentro do perímetro da organização e incluem l*ogs* do *firewall*, sistema de Gerenciamento e Correlação de Eventos de Segurança (SIEM), Sistema de Prevenção de Intrusão (IPS) ou

Sistema de Detecção de Intrusão (IDS) (BROMILEY, 2016).

Os locais em que são extraídos os dados para alimentar as ferramentas automatizadas de Inteligência de Ameaças Cibernéticas são referenciados como *feed* (AZEVEDO, 2020).

Feeds podem ser abertos, obtidos de forma gratuita, tais como: informações de órgãos de segurança de Estados, blogs de fornecedores, informações da *darknet*[5] e os oriundos de OSINT (Inteligência de Fonte Aberta). O *feeds* de OSINT são informações consolidadas de monitoramento de atividades de invasores realizada por uma organização e são muito semelhante aos *feeds* privados (AZEVEDO, 2020; BROMILEY, 2016) .

Feeds privados são aqueles fornecidos mediante pagamento para acesso às bases de inteligência de ameaças, como as que são ofertadas pelas empresas *McAfee e Symantec* (AZEVEDO, 2020).

Fontes externas podem alertar a organização quanto a ameaças não previstas e adicionalmente prover um contexto que ela não tenha, enquanto fontes internas fornecem informações de maior relevância por retratar o quadro atual da instituição.

A integração das informações de inteligência de ameaças internas e externas pode diminuir o intervalo entre as fases de infecção e detecção e de detecção e remediação (BROMILEY, 2016).

Devido à complexidade do fluxo de produção da inteligência, diversas ferramentas foram desenvolvidas no mercado para dar suporte ao processo de inteligência de ameaças cibernéticas.

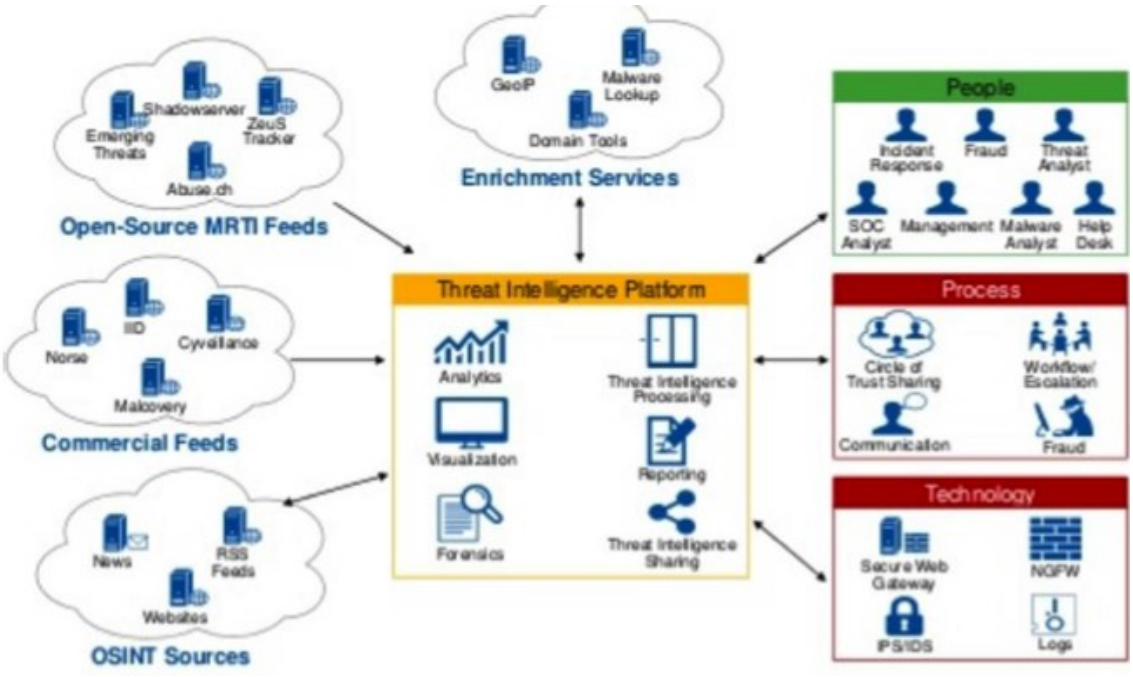
3.3 Plataformas de Inteligência de Ameaças Cibernéticas

Ferramentas conhecidas como Plataformas de Inteligência de Ameaças e referenciadas como na literatura como TIP (*Threat Intelligence Platforms*), facilitam o gerenciamento do conhecimento das ameaças ao integrar informações geradas pela própria organização com informações geradas por fontes externas, enriquecendo a análise e auxiliando na tomada de decisão (SILVA, 2020). A figura 2 ilustra a integração de fontes internas e externas de dados com uma Plataforma de Inteligência de Ameaças Cibernéticas e

5 Rede acessada somente por meio de *software* específico e que tem como característica o anonimato dos usuários que a utilizam (elaborado pela autora).

o compartilhamento da Inteligência com diferentes atores da estrutura de defesa organizacional.

Figura 2 - Plataforma de Inteligência de Ameaças Cibernéticas



Fonte: EUROPEAN UNION (EU) (2017, p. 8).

Algumas soluções são de código aberto, ou seja, podem ser distribuídas, utilizadas e modificadas de forma livre. Dentre elas, destacam-se:

— *Malware Information Sharing Platform* (MISP): possui um banco de indicadores de comprometimento (IOCs) com informações técnicas de ameaças cibernéticas que podem ser compartilhadas e correlacionadas visando a descrição de eventos (SILVA, 2020);

— *Collective Intelligence Framework* (CIF): ao obter informações das fontes, agrupa as ameaças cibernéticas e cria uma sequência cronológica de uma ameaça específica (SILVA, 2020); e

— *Collaborative Research Into Threats* (CRITS): combina mecanismos de análise com um banco de dados de ameaças cibernéticas provendo aos analistas a capacidade de condução de análise e correlação de ameaças (SILVA, 2020).

Sonwani *et al.* (2022) diferenciou as plataformas com base nos seguintes

critérios:

— formato de exportação e importação: refere-se à capacidade de suportar diferentes formatos de dados de ameaças no processo de importação desses dados de fontes, sejam elas internas ou externas, e de exportar dados correlacionados para outros sistemas de segurança. A padronização de dados é um requisito importante para a conformidade da informação entre diferentes sistemas de origem e destino e para o compartilhamento de informações de inteligência de ameaças entre entidades. Dentre os formatos existentes, podemos citar: CybOX, STIX, TAXII, IODEF, RID etc.

— capacidade de integração: diz respeito à integração da plataforma com outras ferramentas de segurança como SIEM e IDS, possibilitando o monitoramento proativo de ameaças;

— suporte à colaboração: atuação da plataforma de forma centralizada ou descentralizada;

— recursos de análise: capacidade analítica da ferramenta de relacionar, priorizar e categorizar as ameaças quanto à urgência. A análise em tempo real é fundamental para responder às ameaças de forma rápida e eficaz;

— geração de gráficos: visualização gráfica do relacionamento de componentes da inteligência de ameaças;

— licença: as plataformas citadas estão disponível sob licença de código aberto; e

— requisitos de *hardware*: MISP e CRITS necessitam recursos de processamento similares enquanto CIF requer recursos mais rigorosos.

Esses critérios foram utilizados para comparar as plataformas com relação ao desempenho. O quadro 2 mostra uma comparação das características das plataformas (MISP, CIF e CRIT) e suas respectivas avaliações nos graus baixo, médio e avançado:

Quadro 2 - Quadro comparativo entre plataformas

Critérios Avaliados	**MISP**	**CIF**	**CRIT**
Formato de Exportação/Importação	*	x	*
Capacidade de Integração	*	*	x
Compartilhamento de Dados	*	x	x

Suporte à Colaboração	*	*	x
Capacidade Analítica	x	x	*
Geração de Gráfico	x	x	*
Licença	*	*	*
Requisitos de Hardware	*	-	*

- baixo x médio * avançado

Fonte: SONWANI *apud* FAIELLA (2019, p. 4).

CTIR e MISP foram as plataformas que tiveram melhor desempenho no quesito de padronização da inteligência de ameaças por meio da importação e exportação de dados em diversos formatos: TAXII, CybOX, OpenIOC, STIX etc (SONWANI, 2022).

MISP e CIF incluem funcionalidades que permitem a integração com ferramentas internas como o IDS (Sistema de Detecção de Intrusão) e SIEM (SONWANI, 2022), sendo que MISP foi considerada a plataforma mais adaptável (SILVA, 2020). Apesar da plataforma CRIT não possuir uma capacidade de integração tão alta quanto à MISP e CIF, seu amplo banco de dados de inteligência de ameaças favorece o desenvolvimento de soluções que permitem essa integração (SONWANI, 2022).

Segundo Silva (2020), muitas organizações dependem das plataformas de código aberto, disponíveis para aprimorar sua capacidade de detecção e prevenção de ameaças cibernéticas. Por não existir uma plataforma de código aberto que atenda todos os processos de Inteligência de Ameaças Cibernéticas, uma forma de ampliar e otimizar os resultados é a integração dessas plataformas.

Por fim, depreende-se que as Plataformas de Inteligência de Ameaças Cibernéticas são uma importante ferramenta na automatização do processo de Inteligência de Ameaças Cibernéticas, auxiliando as organizações no aprimoramento dos mecanismos de defesa na velocidade requerida para enfrentar a rápida evolução das ameaças cibernéticas.

4 PLATAFORMA DE INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS NA MB

Nesta seção será apresentada a forma como é conduzida a Inteligência de Ameaças Cibernéticas pela estrutura de Defesa Cibernética da MB e demonstrado como o

emprego da Plataforma de Inteligência de Ameaças Cibernéticas pode contribuir para a prevenção e mitigação de ameaças, ao automatizar o processo de Inteligência de Ameaças Cibernéticas.

4.1 A Defesa Cibernética no Brasil

O Brasil, por meio da sua Estratégia Nacional de Defesa (END), definiu o setor cibernético como estratégico para a Política Nacional de Defesa (PND) (BRASIL, 2012). Nela, foi atribuída como tarefa para as Forças Singulares, componentes da Estrutura Cibernética de Defesa, a colaboração com as atividades de Inteligência de fonte cibernética em proveito das atividades do Sistema Militar de Defesa Cibernética (SMDC). Coube ainda às Forças Singulares reforçar a proteção das infraestruturas críticas, quando necessário, de forma a garantir o funcionamento diante de ataques cibernéticos.

O SMDC tem como órgão central o Comando de Defesa Cibernética (ComDCiber), cuja finalidade é "garantir a capacidade de atuação em rede, a interoperabilidade dos sistemas e a obtenção dos níveis de segurança necessários, no âmbito da Defesa Nacional", de forma que ela possa atuar em sinergia com as Forças Singulares e respeitando as características intrínsecas dessas, em prol da defesa do ECiber (BRASIL, 2021, p. 49).

Segundo Brasil (2021), a responsabilidade de cada órgão foi definida de acordo com os níveis de decisão ou condução da guerra em que atuam. A figura 3 ilustra a correspondência entre órgãos, nível de decisão em que atuam (tático, operacional, estratégico e político) e responsabilidades (Segurança Cibernética, Defesa Cibernética e Guerra Cibernética).

Figura 3 - Níveis de condução da guerra

Fonte: Brasil (2020, p. 177).

No nível político, a Segurança Cibernética — responsável pela proteção de sistemas e de infraestruturas críticas — é coordenada pela Presidência da República por meio do Gabinete de Segurança Institucional. As diretrizes emanadas por esse órgão envolvem a Administração Pública Federal direta e indireta.

No nível estratégico, a Defesa Cibernética é exercida pelo Ministério da Defesa, Estado-Maior Conjunto das Forças Armadas (EMCFA) e Comandos das Forças Singulares que interagem com outros órgãos participantes da Defesa Nacional.

Os níveis político e estratégico são conduzidos em tempo de paz e orientam como os níveis mais baixos (operacional e tático) devem operar.

Os níveis operacional e tático são empregados em tempo de conflito militar em que a Guerra Cibernética, a cargo dos Comandos Operacionais e Forças Componentes, tem como objetivo alcançar um efeito desejado (BRASIL, 2021).

4.2 A Defesa Cibernética na MB

Devido à transversalidade das ações cibernéticas nos diferentes contextos e níveis decisórios, a MB atua tanto da Defesa Cibernética quanto na Guerra Cibernética.

Conforme já visto nas seções anteriores, as ameaças evoluem em quantidade e em complexidade no intuito de se ocultarem para realizar com sucesso os seus objetivos que vão da espionagem, com a obtenção de informações privilegiadas, à paralisação de sistemas essenciais públicos ou privados.

Identificar e compreender rapidamente as ameaças torna-se essencial para que a Marinha tenha uma adequada consciência situacional do ECiber-MB e possa se preparar com antecedência para o agravamento de uma situação ou uma mudança de contexto da paz para a guerra, com o conflito entre Estados.

Nesse sentido, as atividades de inteligência no campo cibernético, voltadas para o conhecimento e previsão de ameaças, têm se mostrado um importante aliado na preparação da Marinha, pois atua em todos os níveis decisórios e direciona os investimentos necessários para defesa do ECiber-MB.

Preparar-se envolve fortalecer ou investir em novos procedimentos ou

ferramentas de segurança, erradicando ou mitigando vulnerabilidades de acordo com as ameaças que possam emergir no espaço cibernético, bem como os riscos que elas representam. A execução dessas atividades contribuem para resiliência cibernética dos Poderes Naval e Marítimo contra atos de exploração e ataque, além de contribuir para a Segurança Cibernética Nacional, uma vez que a Marinha atua em todos os níveis decisórios.

Com isso, a estrutura de Defesa Cibernética da Marinha deve funcionar de forma dinâmica, com a devida autonomia dos órgãos que a compõem, para que a processo decisório seja tão rápido e assertivo quanto às ações cibernéticas em curso.

Assim, definiu-se a Diretoria-Geral do Material da Marinha (DGMM) como responsável pela normatização dos assuntos referentes às atividades de monitoramento, prevenção, operação, manutenção e proteção do ECiber-MB. A execução dessas atividades é realizada por todas as OM da MB que são coordenadas e orientadas pela Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), a fim de garantir que essas atividades estejam em conformidade com as normas emanadas.

Coube ainda à DCTIM a execução de atividades que visam à prevenção e proteção do ECiber-MB por meio do emprego de adequadas ferramentas e técnicas que protejam redes e sistemas das ações de exploração ou ataque de ameaças bem como a coordenação e orientação das atividades do Centro de Tecnologia da Informação da Marinha (CTIM).

A Marinha, na figura da Diretoria-Geral de Navegação, também possui como responsabilidade a elaboração de normas e orientações com o objetivo de proteger as infraestruturas críticas do Poder Marítimo (BRASIL, 2021).

No contexto de guerra, o Comando Naval de Operações Especiais (CoNavOpEsp) constituirá Grupamentos Operativos de Guerra Cibernética (GptOpGCiber) para atuar nos níveis tático e operacional de acordo com o planejamento operacional, diretivas e Regras de Engajamento divulgadas pelo Comando de Operações Navais (ComOpNav) (BRASIL, 2021). Essas diretrizes serão elaboradas de forma a enfrentar a ameaça real, portanto, conhecer suas Táticas, Técnicas e Procedimentos (TTP) é primordial para entender a finalidade da ameaça e estabelecer estratégias que inviabilizem o seu sucesso.

As atividades de Inteligência no campo cibernético ficaram a cargo do Centro de Inteligência da Marinha (CIM) responsável também pela divulgação de orientações nessa

área (BRASIL, 2021). A Inteligência Cibernética utiliza outras disciplinas na área de segurança da informação, dentre elas, a Inteligência de Ameaças.

Tanto a Inteligência Cibernética quanto as medidas de Contra-Inteligência, conduzidas pelo CIM, podem eventualmente serem apoiadas pelo CoNavOpEsp, DCTIM e CTIM quando houver a necessidade de combater uma ameaça que tem por objetivo comprometer o ECiber-MB (BRASIL, 2021). Logo, percebe-se a importância das OM envolvidas possuírem a mesma visão e entendimento das ameaças desde o tempo de paz para quando houver a mudança do alarme cibernético devido a elevação de risco de um ataque, ou até mesmo uma mudança de contexto para o de conflito, todos estejam adequadamente preparados para executar as ações de defesa necessárias para proteger o ECiber-MB.

Nesse sentindo, a forma como é conduzida a Inteligência de Ameaças Cibernéticas é um fator preponderante para a previsão de ameaças, mitigação das vulnerabilidades, planejamento em conjunto das ações necessárias em caso de um ataque cibernético e investimentos nas ferramentas e mecanismos de proteção de sistemas. Ademais, o conhecimento obtido das ameaças podem também ser compartilhados com o SMDC, proporcionado não somente o fortalecimento do ECiber-MB como também da segurança nacional como um todo.

4.2.1 A Inteligência de Ameaças Cibernéticas na MB

Considerando o crescimento constante das ameaças em quantidade e sofisticação e a necessidade de conhecimento dessas ameaças, a DCTIM estabeleceu, em seu boletim técnico, procedimentos para realização da Inteligência de Ameaças Cibernéticas por meio de relatório denominado Relatório de Inteligência de Ameaças Cibernéticas (RIAC). O relatório consolida informações de ferramentas de gerenciamento e segurança de redes de computadores, proporcionando um conhecimento a respeito das motivações, intenções e métodos utilizados por ameaças cibernéticas internas ou externas à organização (BRASIL, 2018).

Dentre as ferramentas adotadas pela MB, mencionadas no referido boletim técnico, podemos citar: *Firewall*, Sistema de Prevenção de Intrusão (IPS), *Data Loss*

Prevention (DLP)[6], *Web Gateway*[7], Sistema de Gerenciamento de Correlação de Eventos (SIEM), antivírus e fontes abertas.

O compartilhamento do conhecimento do relatório, fruto da consolidação das informações geradas pelas ferramentas de gerenciamento e segurança de rede, é realizado mensalmente pelo CTIM com a DCTIM.

O acompanhamento por meio de relatórios permite a obtenção de um panorama sobre a consciência situacional cibernética da MB, identificando os riscos e probabilidades de ataques cibernéticos que permitam à MB decidir sobre a necessidade de alteração do nível de alarme cibernético, que corresponde à probabilidade de ataques direcionados à MB. Além disso, possibilita o auxílio nas tomadas de decisões que envolvam estratégias de proteção de redes e sistemas do espaço cibernético da Marinha. Os relatórios são analisados nos níveis tático, operacional e estratégico.

No nível tático, o Centro de Tratamento de Incidentes de Redes da MB coleta subsídios para prever ataques cibernéticos que explorem vulnerabilidades já identificadas, possibilitando a definição de ações que promovam a mitigação dessas vulnerabilidades e o fortalecimento da defesa contra ataques cibernéticos.

No nível operacional, os Departamentos de SIC (Segurança da Informação e Comunicações) e conectividade da DCTIM e CTIM utilizam o relatório para compreensão das vulnerabilidades e ameaças que permeiam o ECiber-MB, auxiliando o decisor a propor melhorias para a defesa.

No nível estratégico, o Diretor da DCTIM toma decisões com o fim de aperfeiçoar a política de segurança das informações digitais na MB e proporcionar as condições ideais para que os níveis tático e operacional cumpram com suas atribuições.

O CIM contribui para a Inteligência de Ameaças ao realizar a Inteligência de Fontes Abertas (OSINT).

A OSINT é um tipo de inteligência que coleta, processa e correlaciona informações oriundas de fontes de informações gratuitas e acessíveis para gerar conhecimento e proporcionar linhas de ação contra ameaças (GARLINDO, 2020). Destacam-se dentre as fontes: redes sociais, informações públicas de governos, trabalhos, sítios de

6 Sistema que previne a perda ou exfiltração de dados (elaborado pela autora).
7 Sistema de filtragem de tráfego malicioso da Internet (elaborado pela autora).

busca, fóruns e *deepweb*[8]. Para não comprometer o conhecimento a ser obtido pela OSINT, as fontes devem ser checadas quanto a sua qualidade e confiabilidade.

De fato, a Marinha realiza a Inteligência de Ameaças Cibernéticas, todavia nota-se que o processo estabelecido não está automatizado. O tempo levado para a consolidação do conhecimento e compartilhamento dos relatórios é relativamente alto se considerarmos a velocidade com que as ameaças evoluem, impactando nas ações para mitigar vulnerabilidades e outras ações necessárias para evitar um ataque cibernético. Durante a pesquisa, não foram encontrados indícios da existência de uma plataforma de inteligência de ameaças cibernéticas.

Destarte, o uso de Plataforma de Inteligência de Ameaças Cibernéticas tem se mostrado eficaz na produção, análise e compartilhamento do conhecimento de ameaças ao automatizar o gerenciamento de inteligência de ameaças, simplificando grande parte do trabalho realizado por instituições que a empregam.

4.2.2 Emprego da Plataforma de Inteligência de Ameaças Cibernéticas na MB

A Plataforma de Inteligência de Ameaças pode proporcionar à MB um programa de Inteligência de Ameaças único, capaz de suprir as necessidades de uso de cada nível decisório. A sua capacidade de integração com fontes variadas pode ser explorada pela Força Naval: fontes oriundas de ferramentas OSINT do CIM, de ferramentas de gerenciamento de segurança, utilizadas pelo CTIM, ou da *deepweb/darkweb*[9] explorada pelo CoNavOpEsp; proporcionando o enriquecimento do conhecimento a ser produzido pela plataforma e, consequentemente, o mapeamento correto da ameaça. Fontes da Internet também podem ser integradas, aumentado o volume de informações de ameaças. Quanto maior o volume de informação, mais alta é a capacidade de detecção e previsão de ameaças.

Detalhes técnicos da ameaça, tais como a sua origem, chamados de indicadores de comprometimento, são centralizados num único ambiente criando uma verdadeira enciclopédia das ameaças. Dessa enciclopédia de ameaças, o Centro de Tratamento de Incidentes de Redes da MB obteria indicadores e amostras de *malwares* fruto do resultado de análises profundas de investigação e forense de *malware*.

---

8 Internet em que as páginas web não são indexadas pelos mecanismos de busca (elaborado pela autora).

9 Parcela da rede da *deepweb* comumente utilizada para prática de crimes (elaborado pela autora).

O uso da plataforma altera a postura das organizações, de reativa para proativa, sinalizando problemas emergentes no cenário de ameaças, recomendando mitigações e auxiliando as ações necessárias quando da ocorrência de um incidente de segurança.

Portanto, o emprego por todas as OM partícipes da estrutura de defesa cibernética da MB, ao mesmo tempo, forneceria informações importantes sobre os atores de ameaças, suas intenções, táticas e seus prováveis alvos, trazendo agilidade na tomada de decisão em cada nível decisório.

As equipes de operações de segurança do CTIM processariam melhor o fluxo de alertas de diferentes ferramentas de gerenciamento de segurança, pois isso seria feito de forma automática pela plataforma, priorizando e filtrando os alertas e outras ameaças.

Departamentos de SIC e conectividade da DCTIM e CTIM conseguiriam identificar com maior rapidez as vulnerabilidades de alto impacto nos ativos da MB sujeitas à exploração, optando pela correção dessas vulnerabilidades.

Um outro benefício da plataforma é o auxílio na diferenciação das ameaças imediatas em relação às ameaças potenciais, ao considerar o contexto externo. O conhecimento das ameaças potenciais proporcionaria um planejamento melhor das ações ofensivas e o direcionamento para qualificação necessária do CoNavOpEsp e dos GptOpGCiber para o enfrentamento dessas ameaças. Ademais, mitigaria os impactos advindos da mudança do tempo de paz para o de guerra ao reduzir a probabilidade do fator surpresa.

O conhecimento produzido pela MB poderia ser inclusive compartilhado com terceiros, como outra Força Singular ou ComDCiber, sendo uma importante arma para o combate de ameaças sofisticadas como a APT e *Zero-Day*, contribuindo sobremaneira para segurança das infraestruturas críticas nacionais.

Por mais que a implantação de uma plataforma possa trazer um novo ganho nas estratégias necessárias para defesa frente a evolução constante das ameaças, ainda sim não consegue cobrir todos os escopos. As lacunas de conhecimento e habilidades das organizações da MB seriam superadas através do compartilhamento do conhecimento sobre ameaças com outras organizações, permitindo um aprimoramento dos mecanismos de defesa contra ataques cibernéticos. Neste caso, o desafio está em consolidar informações de fontes heterogêneas para produzir o conhecimento necessário e padronizar esses dados

para que ele seja compreensível e compartilhável. É também uma oportunidade para compartilhar não somente a inteligência conquistada como também as melhores práticas e lições aprendidas.

A escolha de uma determinada plataforma de inteligência de ameaças cibernéticas deve ser precedida do entendimento das necessidades de conhecimento da MB e pela definição dos requisitos automatizados de coleta e processamento de inteligência. É uma etapa importante para maximizar todos os benefícios que podem ser proporcionados pela plataforma.

Uma boa linha de ação é iniciar a automatização da inteligência de ameaças cibernéticas com a adoção de uma plataforma de inteligência de ameaças gratuita (*open source*) e integrá-la com ferramentas de gerenciamento de segurança, como o SIEM por exemplo. Para uma abordagem mais completa, é possível a integração com outras plataformas gratuitas.

Após a definição dos requisitos e da estimativa do volume de dados necessários para produção do conhecimento, a MB pode decidir por manter a plataforma gratuita, escolher adquirir uma plataforma comercial paga tendo como base experiência prévia com o uso da plataforma gratuita ou desenvolver uma. O desenvolvimento de uma plataforma para MB deve considerar a formatação dos dados utilizada por outras plataformas no âmbito do Ministério da Defesa, caso exista, a fim de facilitar o compartilhamento do conhecimento.

Por fim, o emprego de uma plataforma de inteligência de ameaças cibernéticas permite a visualização estruturada, por meio de gráficos, das ameaças imediatas e a previsão de novas ameaças dentro do contexto que a organização está inserida, fornecendo métricas e indicadores que auxiliarão nas ações de defesa da MB.

Plataformas de Inteligência de Ameaças Cibernéticas utilizam a mesma fonte das ameaças: a Internet. Enquanto essas evoluem num ritmo acelerado no intuito de aperfeiçoar os ataques cibernéticos, àquelas a usam para prever os atores aptos a lançar ataques tendo como alvo a organização em questão.

5 CONCLUSÃO

Conclui-se que o estabelecimento do setor cibernético como estratégico na

Política Nacional Defesa trouxe, como desafio para MB, a tarefa de aprimoramento constante da sua defesa cibernética para combater ameaças em evolução.

O Brasil tem se destacado como um dos principais países alvo de ataques cibernéticos no mundo. O número de ataques cresce numa curva exponencial e impacta serviços essenciais e infraestruturas críticas, causando prejuízos que chegam ao triplo do Produto Interno Brasileiro (PIB).

A MB possui um importante papel na segurança nacional por ser responsável por orientar a proteção das infraestruturas críticas do Poder Marítimo e por contribuir com o SMDC.

Estados, terroristas, ativistas e criminosos são algumas das ameaças por trás dos ataques cibernéticos que, para driblar as ferramentas de segurança, costumam utilizar técnicas complexas e sofisticadas que evoluem em ritmo acelerado para permanecerem ocultas até que seus objetivos sejam alcançados.

Diante desse fato, práticas tradicionais, tais como: métodos simples de monitoramento humano de ameaças, utilização de dispositivos de segurança comuns e de indicadores baseados em incidentes de segurança que já ocorreram, são eficazes apenas para conter ataques cibernéticos generalizados, pois não levam em consideração o contexto organizacional.

Logo, apesar de haver certo nível de maturidade da Força Naval ao empregar a inteligência de ameaças cibernéticas por meio de relatórios — que consolidam informações sobre ameaças, priorizando-as, fruto dos resultados obtidos pelas ferramentas de segurança — e do uso de ferramentas de OSINT; ainda sim, há necessidade de uma tecnologia para automatizar esse processo e contextualizá-lo.

A Plataforma de Inteligência de Ameaças Cibernéticas surge como uma solução de automatização e integração da inteligência de ameaças internas e externas, capaz de prever ameaças potenciais, direcionar esforços e investimos para mitigar as vulnerabilidades e apoiar na tomada de decisão.

Caso seja adotada no âmbito interno, poderá ser aproveitada por todas as organizações que compõem a estrutura de Defesa Cibernética e em todos os níveis decisórios, agilizando a comunicação entre as partes e reduzindo o tempo necessário para priorizar os riscos.

O compartilhamento do conhecimento produzido com terceiros reduz as lacunas de conhecimento e contribui para o fortalecimento da segurança nacional, no entanto faz-se necessária a padronização do formato dos dados a fim de que haja uma interoperabilidade com outras plataformas já estabelecidas na esfera governamental.

Para que a plataforma desempenhe um papel significativo, ela deve se adequar às necessidades e requisitos previamente definidos pela MB. Por isso, recomenda-se inicialmente o uso de plataformas de inteligência de ameaças de código aberto para que a instituição se familiarize com a tecnologia antes de realizar um investimento financeiro para adquirir uma plataforma comercial paga ou optar pelo desenvolvimento de uma.

Ao alcançar o estado da arte, a plataforma de inteligência de ameaças cibernéticas na MB será capaz de: identificar e prever ataques cibernéticos sofisticados de ameaças, inferindo como elas podem surgir, detectar atividades que podem indicar um ataque direcionado, responder mais rapidamente aos ataques com melhores contramedidas e fechar as brechas de segurança para reduzir os riscos de exfiltração de dados e interrupção dos serviços.

Com a mudança de uma postura reativa para uma proativa, o emprego da plataforma de inteligência de ameaças pela estrutura de defesa cibernética da MB tornará eficaz a detecção e previsão de ameaças do ECiber-MB, além de fortalecer a defesa dos ativos de interesse.

REFERÊNCIAS

AHLBERG, Christopher. **The Threat Intelligence book - Moving toward a security intelligence program**. [s.l.]: Cyberedge Press, 2019. 94p.

AVELAR, José Ricardo Cabral. **A Guerra Cibernética e seus desafios para o Brasil**. 2018. Trabalho de Conclusão de Curso (Pós-graduação lato sensu) - Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2018. 74f.

AZEVEDO, Bruce William Percílio**. Modelo de referência para o desenvolvimento de aplicações de inteligência de ameaças cibernéticas e sua aplicabilidade para o compartilhamento de dados.** 2020. Dissertação (Mestrado Profissional em Engenharia Elétrica) - Universidade de Brasília, Brasília, 2020. 77f.

BARBOSA, Andressa. Especialistas alertam para os principais ataques cibernéticos de 2022. **Forbes**, São Paulo, 2 de fev. de 2022. Disponível em: <https://forbes.com.br/forbes-tech/2022/02/os-principais-ataques-ciberneticos-previstos-para-2022/>. Acesso em: 25 de mai. de 2022.

BARNUM, Sean. **Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX)**. 2012. 22p. Disponível em: <https://www.mitre.org/publications/technical-papers/standardizing-cyber-threat-intelligence-information-with-the>. Acesso em: 15 jun. 2022.

BRASIL. Estado-Maior da Armada. **Doutrina cibernética da Marinha.** Brasília, 2021. 117p.

BRASIL. Estado-Maior Conjunto das Forças Armadas. **Doutrina Militar de Defesa Cibernética**. Brasília, 2014. 38p.

BRASIL. Ministério da Defesa. **Doutrina de Operações Conjuntas - MD30-M-01.** Brasília, DF, 2020. 240p. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md30-m-01-vol-1-2a-edicao-2020-dou-178-de-15-set.pdf>. Acesso em: 18 jul. 2022.

BRASIL. Diretoria de Comunicações e Tecnologia da Informação da Marinha. **DCTIMBOTEC 30/002/2018:** Procedimentos operacionais para elaboração do Relatório de Inteligência de Ameaças Cibernéticas (RIAC). Rio de Janeiro, RJ, 2018. 10p.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro verde:** segurança cibernética no Brasil. Brasília: GSIPR/SE/DSIC, 2010. 63p.

BROMILEY, Matt. **Threat Intelligence:** what it is, and how to use it effectively. 2016. Disponível em:

<https://nsfocusglobal.com/wp-content/uploads/2017/01/SANS_Whitepaper_Threat_Intelligence__What_It_Is__and_How_to_Use_It_Effectively.pdf>. Acesso em: 15 jun. 2022.

BBC. **EUA espionaram Petrobras, dizem papéis vazados por Snowden**. Brasília, 8 de setembro de 2013. Disponível em: <https://www.bbc.com/portuguese/noticias/2013/09/130908_eua_snowden_petrobras_dilma_mm>. Acesso em: 22 de mai. de 2022.

COSTA, Matheus. O que é DoS e DDoS?. **Canaltech**, São Paulo, 06 de out. de 2014. Disponível em: <https://canaltech.com.br/produtos/o-que-e-dos-e-ddos/>. Acesso em: 25 de mai. de 2022.

CNN. **Sistemas do Ministério da Saúde estão fora do ar após tentativa de invasão**. São Paulo, 17 de maio de 2022. Disponível em: <https://www.cnnbrasil.com.br/saude/sistemas-do-ministerio-da-saude-estao-fora-do-ar-apos-tentativa-de-invasao/>. Acesso em: 22 de mai. de 2022.

CLARKE, Richard A.; KNAKE, Robert K. **Guerra Cibernética:** a próxima ameaça à segurança e o que fazer a respeito. [s.l.]: Brasport, 2010. 257p.

CISOMAG**. Everything You Need to Know About the Evolution of Cyberthreats**. Albuquerque – NM, 16. ago. 2021. Disponível em: <https://cisomag.eccouncil.org/the-evolution-of-cyberthreats/ >. Acesso em: 25 de mai. de 2022.

DUTRA, André Melo Carvalhais. Introdução à Guerra Cibernética: a necessidade de um despertar brasileiro para o assunto. **IX Simpósio de Guerra Eletrônica** - Instituto Tecnológico da Aeronáutica, São José dos Campos, 2007.

EUROPEAN UNION (EU). European Union Agency For Network and Information Security. **Exploring Oportunities and limitations of current Threat Intelligence Platforms**. Version 1. 2017.

FOLHA. **Ataque hacker que atingiu Microsoft e setor militar dos EUA destrói ilusão de segurança na rede**. São Paulo, 29 de jan. de 2021. Disponível em: < https://www1.folha.uol.com.br/ilustrissima/2021/01/ataque-hacker-que-atingiu-microsoft-e-setor-militar-dos-eua-destroi-ilusao-de-seguranca-na-rede.shtml>. Acesso em: 20 de abr. de 2022.

FRIEDMAN, Jon; BOUCHARD, Mark. **Definitive guide to cyber threat intelligence:** using knowledge about adversaries to win the war against targeted attacks. 2015. 74p.

FLASHPOINT TEAM. Flashpoint, 2022. **Guide to Cyber Threat Intelligence:** elements of an effective threat intel and cyber risk remediation program. Disponível em: <https://flashpoint.io/blog/guide-to-cyber-threat-intelligence/>. Acesso em: 15 jun. 2022.

FAIELLA, Mario et al. Enriching Threat Intelligence Platforms Capabilities. In: 16th INTERNATIONAL CONFERENCE ON SECURITY AND CRYPTOGRAPHY. **Anais. Prague, Czech Republic:** 2019. p. 1-12.

FERNANDES, José Pedro Teixeira. A ciberguerra como nova dimensão dos conflitos do século XXI. **Relações Internacionais**, n. 33, p. 53-69, mar. de 2012.

GARLINDO, Javier et al. **The Not Yet Exploited Goldmine of OSINT:** opportunities, open Challenges and future trends, p. 1-23, 9. jan. 2020. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8954668>. Acesso em: 18 jul. 2022.

KOTTASOVÁ, Ivana. Como as ameaças russas fizeram da Estônia um país especialista em cibersegurança. **CNN**, São Paulo, 19 de jun. 2021. Disponível em: <https://www.cnnbrasil.com.br/business/como-as-ameacas-russas-fizeram-da-estonia-um-pais-em-especialista-ciberseguranca/>. Acesso em: 25 de mai. de 2022.

KLINCZAK, Marjori. Uso da Inteligência na Detecção de Ameaças Cibernéticas. In: THE ELEVENTH INTERNATIONAL CONFERENCE ON FORENSIC COMPUTER SCIENCE AND CYBER LAW. **Anais**. São Paulo: 2019. p. 15-22. Disponível em: <http://icofcs.org/2019/ICoFCS2019-002.pdf>. Acesso em: 15 jun. 2022.

KASPERSKY. **O que são vírus de computador e worm de computador?**. São Paulo, 2022. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/computer-viruses-vs-worms>. Acesso em: 25 de mai. de 2022.

LI, Yuchong; LIU, Qinghui. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. **Energy Reports**, v. 7, p. 8176-8186, 2021.

MOTA, Dardano do Nascimento; MOTA, Fernanda Antônia Barbosa da. Uma proposta do relacionamento entre a Guerra Cibernética e o Terrorismo no contexto informacional e seus reflexos para as infraestruturas críticas. **Revista da Escola Superior de Guerra**, v. 34, n. 71, p. 59-79, mai/ago de 2019.

MCMILLAN, Rob. **Definition:** threat intelligence. Gartner Research, 2013. Disponível em: <https://www.gartner.com/en/documents/2487216>. Acesso em: 15 jun. 2022.

PINTO, Danielle Jacon Ayres; GRASSI, Jéssica Maria. Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil. **Revista Brasileira de Estudos de Defesa**, v. 7, ed. 2, p. 103-131, 22 fev. 2021.

PARKS, Raymond C.; DUGGAN, David P. Principles of Cyberwarfare. **IEEE Security and Privacy Magazine**, v. 9, n. 5, p. 30-35, 26 set. 2011. Disponível em: <https://www.researchgate.net/publication/224259524_Principles_of_Cyberwarfare>. Acesso em: 25 maio 2022.

SÁ, Alan et al. O Encontro da Guerra Cibernética com as Guerras Eletrônica e Cinética no Âmbito do Poder Marítimo. **Revista da Escola de Guerra Naval**, v. 25, n. 1, p. 89-128, jan/abr de 2019.

SHAKARIAN, Paulo. **Stuxnet:** cyberwar revolution in military affairs. SMALL WARS JOURNAL, p. 1-10, 14 abr. 2011. Disponível em: <https://smallwarsjournal.com/blog/journal/docs-temp/734-shakarian3.pdf>. Acesso em: 22 maio 2022.

SHEETER, Laura. Estônia acusa Rússia de 'ataque cibernético' ao país. **BBC,** Brasília, 17 de mai. de 2007. Disponível em:<https://www.bbc.com/portuguese/reporterbbc/story/2007/05/070517_estoniaataques internetrw> Acesso em: 25 de mai. de 2022.

SILVA, Alessandra de Melo e. **Metodologia integrativa para produção de inteligência de ameaças cibernéticas utilizando plataformas de código aberto**. 2020. Dissertação (Mestrado Profissional em Engenharia Elétrica) - Universidade de Brasília, Brasília, 2020. 72f.

SILVA, Júlio Cezar Barreto Leite da. Guerra cibernética: a guerra no quinto domínio, conceituação e princípios. **Revista da Escola de Guerra Naval**, v. 20, n.1, p. 193-211, jan/jun de 2014.

SONWANI, Himanshu et al. **A comprehensive study on threat intelligence platform**. In: INTERNATIONAL CONFERENCE ON COMMUNICATION, COMPUTING AND INTERNET OF THINGS (IC3IoT). **Anais**. Chennai, India: 2022. p. 1-5.

SUPER INTERESSANTE. **Tem boi na linha: hackers, os espiões cibernéticos**. São Paulo, 31 de out. 2016. Disponível em: <https://super.abril.com.br/tecnologia/tem-boi-na-linha-hackers-os-espioes-ciberneticos/>. Acesso em: 25 de mai. de 2022.

TIDY, Joe. Guerra na Ucrânia: os três ciberataques russos que as potências ocidentais mais temem. **BBC**, Brasília, 27 de mar. de 2022. Disponível: <https://www.bbc.com/portuguese/internacional-60843427>. Acesso em: 25 de mai. de 2022.

TOUSIN, Wien; RAIS, Helmi. A survey on technical threat intelligence in the age of sophisticated cyber attacks. **Computers & Security**, v. 72, p. 212-233, jan. 2018. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0167404817301839> Acesso em: 4 abr. 2022.

UNITED KINGDOM (UK). National Cyber Security Centre. **Cyber threat intelligence in government:** a guide for decision makers & analysts. 2° version. 2019.

VEJA. **Vazamento de e-mails sugere possível ajuda de Putin a Trump**. Rio de Janeiro, 25 de jul. de 2016. Disponível em: <https://veja.abril.com.br/mundo/vazamento-de-e-mails-

sugere-possivel-ajuda-de-putin-a-trump/>. Acesso em: 19 de abr. de 2022.

ZETTER, Kim. **Countdown to Zero Day:** stuxnet and the launch of the world's first digital weapon. Crown, 2014. 433p.