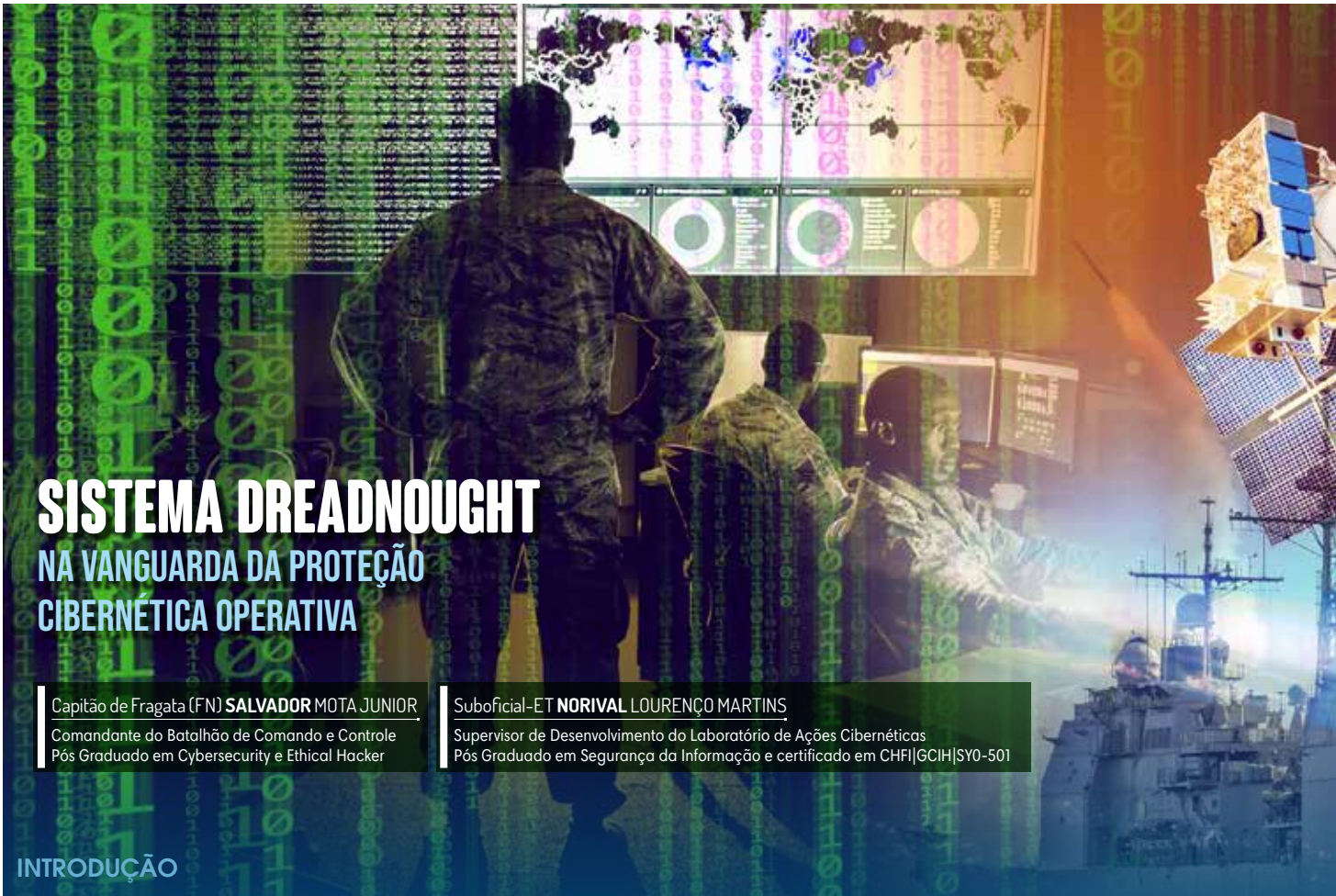

SISTEMA DREADNOUGHT
NA VANGUARDA DA PROTEÇÃO CIBERNÉTICA OPERATIVA

Capitão de Fragata (FN) **SALVADOR** MOTA JUNIOR
Comandante do Batalhão de Comando e Controle
Pós Graduado em Cybersecurity e Ethical Hacker

Suboficial-ET **NORIVAL** LOURENÇO MARTINS
Supervisor de Desenvolvimento do Laboratório de Ações Cibernéticas
Pós Graduado em Segurança da Informação e certificado em CHFI|GCIH|SY0-501

INTRODUÇÃO

Cibernética, hoje, está em todo lugar. Filmes, séries, documentários, livros e cursos procuram aderência ao termo. O uso deste remete a uma mistura de tecnologia de ponta, alta velocidade e valor agregado. O Espaço Cibernético surge a partir da interação entre três componentes vitais: infraestrutura de Tecnologia da Informação, sistemas e usuários. Um espaço virtual é composto pelo conjunto de canais de comunicação da Internet e outras redes de comunicação que garantam a interconexão de ativos informacionais. Engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, o processamento e o compartilhamento de conteúdo – além de todas as ações humanas ou automatizadas. O espaço pode ser desdobrado em camadas. A grande parte das referências utilizadas neste artigo utiliza três estratos: físico, lógico e das identidades virtuais.

A expansão do Espaço Cibernético (ECiber) foi exponencial. Usufruindo dos resultados da 3ª Revolução Industrial, dos avanços tecnológicos, das mudanças sociais e da franca difusão da Internet, o ECiber alcançou uma taxa de povoamento recorde. Quase tudo em termos de serviços, entretenimento, saúde, compras, relacionamentos e vida financeira já migrou ou está no processo de se estabelecer nesse ambiente. Máquinas, programas e pessoas interagindo quase em tempo integral. Esse quadro geral leva o Espaço Cibernético a romper como fator relevante na análise do ambiente operacional. O auge desse raciocínio foi atingido em 2016, quando a Otan passou a considerar o Espaço Cibernético como o 5º Domínio Operacional, junto dos já consagrados domínios Marítimo, Terrestre, Aéreo e Espacial.

E, como não podia deixar de ser, no 5º Domínio também se faz guerra, Guerra Cibernética. Caracterizada pelo uso ofensivo e defensivo de Informação e Sistemas de Informação com a intenção de negar, explorar, corromper, degradar ou destruir capacidades de Comando e Controle do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Abrange, essencialmente, as ações cibernéticas que são do tipo Proteção, Exploração e Ataque.

Com o intuito de oferecer Proteção Cibernética aos meios Navais e de Fuzileiros Navais, em um contexto operativo, foi desenvolvido por militares do Comando Naval de Operações Especiais (CoNavOpEsp) o Sistema *Dreadnou-*

Foto: J.M. Eddins Jr., *U.S. Air Force - U.S. Navy* - www.atoponline.com
Composição Fotográfica: 1°SG Severiano

ght, uma combinação de *hardware* robusto e escalável com *software* livre, modular e customizável.

Inicialmente, vamos conhecer o Sistema *Dreadnought* relatando breve histórico do desenvolvimento do sistema e apontando suas possibilidades e limitações. Em seguida, compreenderemos sua importância, descrevendo o emprego do *Dreadnought* nas operações e nos exercícios. Por fim, analisaremos algumas ações futuras que podem impactar a contraposição às ameaças cibernéticas no nível operacional e tático, examinando os principais desafios na busca pelo emprego eficiente e eficaz do Sistema.

HISTÓRICO

A característica do Poder Naval PERMANÊNCIA indica a capacidade de operar, continuamente, com independência e por longos períodos, em áreas distantes e de grandes dimensões. Para estabelecer comunicação com a Rede de Comunicação Integrada da Marinha (RECIM), os meios navais utilizam *link* satelital nas bandas Ku e X. Duas preocupações serviram de força motriz para o desenvolvimento do Sistema *Dreadnought*:

- Elevado consumo de banda dos *links* satelitais durante as comissões, resultando em péssimo serviço de acesso às páginas da Intranet; e
- Ausência de ferramenta de proteção cibernética para os *links* satelitais e ativos informacionais que permita a identificação, o bloqueio e o reporte das ameaças.

Buscou-se solucionar o primeiro problema implementando um repositório para update do antivírus em uma Estação de Trabalho no próprio navio. Essa medida reduziu o consumo de banda, pois apenas uma Estação usava o *link* para atualização, oferecendo, em seguida, o serviço de *update* do antivírus às demais Estações de Trabalho da rede. Contudo, o Espaço Cibernético continuava sem contar com uma ferramenta robusta para proteger os *links* satelitais e os ativos informacionais críticos durante as comissões.

No ano de 2015, a Divisão de Guerra Cibernética (DivGCiber) integrante, à época, do Comando de Operações Navais (ComOpNav) iniciou a busca por uma solução técnica baseada em ***software*** livre, de baixo custo, de interface amigável, adaptável a qualquer seguimento de rede, de fácil instalação e configuração e que oferecesse aos meios operativos a capacidade de se contrapor às ameaças cibernéticas e de trazer otimização do *link* satelital por meio de um sistema instalado nos meios operativos.

Em 2017, a DivGCiber desenvolveu a versão 1.0 beta do Sistema *Dreadnought*. O nome foi inspirado na classe de Encouraçados do início do século XX. O Encouraçado tinha duas características revolucionárias: um esquema de armamento de calibre único e a propulsão movida por turbinas a vapor. O Sistema *Dreadnought* do Espaço Cibernético oferece também duas respostas às preocupações apontadas acima: otimização no consumo de banda e monitoramento efetivo da rede, permitindo identificar, bloquear e reportar ameaças cibernéticas.

O batismo de fogo do Sistema *Dreadnought* ocorreu no mesmo ano, a bordo da Fragata União, compondo, na época, a Força-Tarefa Marítima (FTM) da Força Interina das Nações Unidas do Líbano (UNIFIL). O sistema foi colocado para monitorar e auxiliar na gerência da rede do navio de forma local e remota, a partir das instalações da DivGCiber. Com o monitoramento, os Operadores Cibernéticos puderam executar as ações de identificação, bloqueio e confecção de reportes. O gerenciamento otimizou o uso da banda e o fluxo de informações no Espaço Cibernético, contribuindo para a construção de uma consciência situacional cibernética.

A partir de então, o ComOpNav passou a ter pleno controle da rede operativa do navio por *link* satelital. No mesmo ano, foram realizados testes junto à Força de Fuzileiros da

Esquadra (FFE), com destaque para as Operações conduzidas em Três Corações/MG e Formosa/GO, com resultados satisfatórios. Em 2018, foi lançada a versão 2.0, que apresentava como diferenciais:

- redução dos requisitos de *hardware*, graças ao desenvolvimento de rotinas e arquitetura de *software* mais inteligentes; e
- capacidade de controle centralizado por painel informativo (dashboard), permitindo o monitoramento das atividades de cada unidade com o Sistema *Dreadnought* em tela única.

Na vanguarda pela proteção cibernética operativa, o Sistema *Dreadnought* continuou experimentando atualizações e aperfeiçoamentos. Em 2019, a DivGCiber passou a conduzir as Ações de Guerra Cibernética a partir do recém ativado CoNavOpEsp. Essa nova Organização Militar tornou-se o centro de desenvolvimento do Sistema *Dreadnought*, lançando a versão 2.4 no mês de abril. Hoje, o Sistema opera em mais de 20 Organizações militares, operativas e administrativas e encontra-se na versão 2.7, que agregou as seguintes funcionalidades:

- *Update* automático de regras do Sistema de Detecção de Intrusão (IDS);
- Otimização da navegação web por *link* satelital (*proxy cache*);
- Armazenamento inteligente dos registros de detecção (Ciclo de Vida do *Log*); e
- Classificação automatizada dos registros de detecção (redução dos falsos positivos).

Suas possibilidades são:

- Segregar o tráfego das redes;
- Realizar análise histórica dos eventos de segurança;
- Identificar, bloquear e reportar ameaças cibernéticas;
- Análise de tráfego em tempo real, de forma local ou remota;
- Exibir tráfego, indicadores de segurança, gráficos e relatórios;
- Construir uma Consciência Situacional a partir do monitoramento do Espaço Cibernético; e
- Agregar funcionalidade à segurança pela robustez, escalabilidade e modularidade do Sistema.

As principais limitações são:

- Não possuir *hardware* proprietário;
- Tratamento de incidentes cibernéticos;
- Análise automatizada do espaço cibernético; e
- Levantamento das vulnerabilidades existentes.

EMPREGO NAS OPERAÇÕES MILITARES

Quando os meios Navais e de Fuzileiros Navais conduzem suas atividades, utilizam diversos sensores para coletar dados sobre o ambiente operacional onde estão inseridos. A fusão desses dados permitirá a confecção de um mosaico panorâmico que entregará informações consistentes, úteis e de alto valor, contribuindo para melhor interpretação da dimensão física, da humana e da informacional do Teatro de Operações.

Com o avanço da Era da Informação, os meios Navais e de Fuzileiros Navais estarão cada vez mais inseridos e dependentes do Espaço Cibernético. Essa afirmação torna-se realidade quando consideramos três aspectos: o aumento do número de sensores destinados à coleta de dados; a complexidade no trabalho de fusão dos dados; e a necessidade de manter fluxo informacional cíclico, veloz e preciso. A combinação desses fatores exigirá que os meios operativos precisem do suporte de ativos computacionais para produzir, processar, compartilhar e armazenar as informações utilizadas na condução de suas operações.

Foto: U.S. Air Force - Paul Shirk

Essa reflexão impulsionou o desenvolvimento do Sistema *Dreadnought*, o qual passou a ser empregado em prol das Operações realizadas com a Esquadra a partir de 2020, entrando no quadro de eventos como Exercício de Contraposição às Ameaças Cibernéticas. Em 2021, passou a ser conduzida também com os

Foto: EBC (Empresa Brasil de Comunicação)

Grupamentos Operativos de Fuzileiros Navais (GptOpFuzNav), organizados pela Força de Fuzileiros da Esquadra (FFE). O exercício ganhou o nome de OCTOPUS, quando realizado com os meios Navais, e ALLIGATOR, quando conduzido junto dos GptOpFuzNav. Busca atingir dois propósitos: aperfeiçoar a execução das ações de guerra cibernética em proveito da Força Naval ou do GptOpFuzNav; e contribuir com a difusão da mentalidade de Proteção Cibernética na MB. Visando atingir os propósitos apresentados acima, o exercício promove:

- Adestramento dos Operadores Cibernéticos a bordo dos navios ou em terra para que, de forma proativa, identifiquem, bloqueiem e reportem as ameaças encontradas no Espaço Cibernético de interesse;
- Adestramento da Divisão de Guerra Cibernética a partir das instalações do CoNavOpEsp para que executem ações do tipo exploração no espaço cibernético de interesse; e
- Construção e expansão da consciência situacional por meio da análise de risco cibernético, resultado da relação entre as ameaças identificadas (probabilidade) e as vulnerabilidades presentes nas camadas do Espaço Cibernético (impacto), a partir dos resultados obtidos.

Dessa maneira, o Sistema *Dreadnought* posiciona-se na vanguarda da proteção cibernética operativa, contribuindo com a contraposição às ameaças cibernéticas que busquem explorar vulnerabilidades existentes no Espaço Cibernético de interesse.

AÇÕES FUTURAS

O desenvolvimento e o emprego do Sistema *Dreadnought* tem revelado alguns desafios que exigirão ações no médio e longo prazo para que o Espaço Cibernético de interesse da MB seja um ambiente controlado, no qual os riscos sejam identificáveis, permitindo a confecção de planos que proponham ações cibernéticas adequadas para tratamento da ameaça, conforme o impacto estimado. Examinaremos três ações futuras que podem impactar a contraposição às ameaças cibernéticas no nível operacional e tático.

Operador Cibernético Dedicado

É de extrema necessidade que se mantenha o Operador Cibernético dedicado na execução das tarefas de identificar, bloquear e reportar uma ameaça cibernética. O Espaço Cibernético é um ambiente dinâmico e traiçoeiro, exigindo que seu monitoramento seja feito de forma plena, com total atenção. Os acontecimentos nesse ambiente, por vezes, são ambíguos e complexos, demandando tempo para análise e, ao mesmo tempo, são voláteis e incertos, impondo que o Operador desenvolva velocidade de raciocínio e *expertise* para não desperdiçar tempo. Mantê-lo dedicado a essa atividade será fundamental para reduzir o risco de uma ameaça identificada explorar com sucesso uma vulnerabilidade existente.

Controle de Avaria Cibernético

Elevar à condição de avaria qualquer incidente cibernético que ocorra no contexto operativo: essa ação observa estreita ligação com a ação anterior, permitindo o desenvolvimento de procedimentos operativos padronizados oriundos

das boas práticas realizadas pelos Operadores Cibernéticos. Além disso, a ação impacta todos os três estratos do Espaço Cibernético, em especial o ser humano responsável pela identidade virtual, que experimentará a transferência de ações cibernéticas sendo representadas como ações cinéticas no mundo real.

Consciência Situacional Cibernética

Um dos maiores desafios para a condução das ações de guerra cibernética é construir e manter em expansão uma Consciência Situacional Cibernética precisa, que seja resiliente às intempéries do ambiente informacional. Essa ação tem sua efetividade atrelada às ações anteriores, visto que trata-se de uma análise constante da situação da rede de computadores e do fluxo de informações utilizadas para apoiar a tomada de decisão. Sem um Operador Cibernético dedicado a classificação dos acidentes cibernéticos como avarias ao meio Naval ou ao GptOpFuzNav, impactando no cumprimento da missão, o Espaço Cibernético não comporá o mosaico da Consciência Situacional.

CONSIDERAÇÕES FINAIS

O Sistema *Dreadnought* é uma solução que fornece a proteção cibernética para os meios operativos que utilizam o Espaço Cibernético para produzir, processar, compartilhar e armazenar as informações utilizadas na condução de suas Operações. Seu histórico mostra que a evolução dos assuntos cibernéticos é constante, exigindo dos Operadores Cibernéticos disciplina e dedicação aos assuntos afetos à área, a fim de que possam acompanhar as tendências globais. A familiaridade com o Sistema permitirá o aproveitamento máximo das suas possibilidades, bem como a adequação necessária ante as limitações inerentes.

O emprego nas operações da Esquadra e dos GptOp-FuzNav tem se mostrado como uma decisão acertada, uma vez que, a cada OCTOPUS / ALLIGATOR, observa-se o aperfeiçoamento dos Operadores Cibernéticos na execução das ações de guerra cibernética do tipo proteção e exploração, além da difusão da mentalidade de Proteção Cibernética na MB. As ações futuras foram visualizadas pelos desafios que surgiram no desenvolvimento e aplicação do Sistema nas operações. Ultrapassar esses desafios permitirá: a consolidação de uma massa crítica sólida e experimentada sobre as questões cibernéticas; a pronta resposta aos incidentes causados pelas ameaças cibernéticas; e o atingimento de níveis sofisticados do fluxo de informações para tomada de decisão considerando o Espaço Cibernético.

O Sistema *Dreadnought* não é um fim em si mesmo, mas parte de um sistema maior, o Sistema Naval de Guerra Cibernética – conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e recursos humanos e financeiros essenciais para a realização de ações de Guerra Cibernética no Espaço Cibernético, assegurando seu uso efetivo pelas Forças Navais e de Fuzileiros Navais, bem como impedindo ou dificultando sua utilização por adversários.

Foto: NAVAL GROUP - www.naval-group.com

REFERÊNCIAS

BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **MD31-M-07**: doutrina militar de defesa cibernética. Brasília, DF: EMCFA, 2014.

MARINHA DO BRASIL. Estado-Maior da Armada. **EMA-419**: doutrina cibernética da Marinha. Brasília, DF: EMA, 2021.

NORTH ATLANTIC TREATY ORGANIZATION. **AJP-3.20**: allied joint doctrine for cyberspace operations. Bruxelas: NATO Standardization Office, 2020.

NORTH ATLANTIC TREATY ORGANIZATION. **NATO glossary of terms and definitions**: AAP-06. Bruxelas: NATO Standardization Office, 2020.