Cibersegurança Naval: navegando em águas turbulentas na era da Guerra Cibernética

9

Capitão-Tenente Warlley **Paulo Freire**

É formado em Ciências Navais pela Escola Naval, com Habilitação em Eletrônica. Em sua trajetória profissional, realizou diversos cursos, com destaque para: Pós-graduação em Segurança das Informações e Comunicações (CIAW/PUC-RIO) e em Guerra Cibernética (CIGE), *Continuous Monitoring and Security Operations* (BASE4 Security) e Inteligência Cibernética (EsIMar). Entre as principais comissões, foi Ajudante do Encarregado da Divisão O-1 na Corveta Júlio de Noronha, Chefe do Departamento de Operações do Navio-Patrulha Fluvial Pedro Teixeira e Encarregado da Divisão O-2 na Fragata Liberal; atualmente, também é Orientador Pedagógico do CAp-A (CIAA).

Introdução

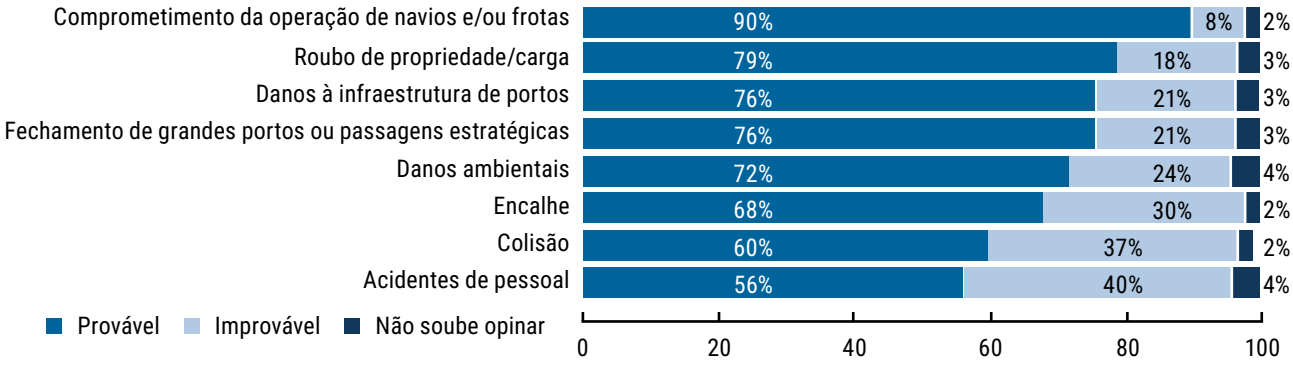
A vertente marítima dos domínios comerciais e militares tem sido a espinha dorsal do comércio internacional e das principais forças de defesa. Segundo o último relatório da Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD, 2022), em 2022 o setor marítimo movimentou onze bilhões de toneladas em bens, o que representa 80% de todo o volume global de comércio. A evolução do setor marítimo, cada vez mais conectado e digitalizado, tem transformado as operações comerciais e militares no mar, aprimorando a eficiência e a efetividade dos meios navais. Todavia, essa evolução também expõe o setor às crescentes ameaças cibernéticas: dados de 2018 a 2021 mostram um crescimento de 900% nos registros de ataques cibernéticos ao setor marítimo (FREIRE et al., 2021).

Nessa conjuntura, os navios vêm se tornando complexos sistemas ciber-físicos que integram sensores, sistemas de informação e sistemas de controle e automação (FREIRE et al., 2022). Muitos dos sistemas a bordo, como navegação, propulsão e comunicação, são integrados por redes digitais, da mesma forma que os portos dependem de complexos sistemas digitais para logística e segurança. No âmbito militar, navios de guerra operam cada vez mais sob a égide da guerra centrada em redes, com sistemas de comunicação satelitais integrando seus diversos sistemas operativos e de comando e controle.

Doravante, nesses complexos sistemas heterogêneos, cada elemento representa uma potencial vulnerabilidade que pode ser explorada em um ataque cibernético, um potencial elo mais fraco nessa extensa cadeia que pode permitir o comprometimento de outros sistemas do setor marítimo (KESSLER; SHEPARD, 2022).

De forma a dimensionar esse risco, a norueguesa DNV, uma das três maiores sociedades classificadoras de navios do mundo, publicou em seu relatório de Prioridades Cibernéticas para o Setor Marítimo em 2023 uma pesquisa envolvendo 801 profissionais do setor distribuídos em 72 países. Entre as estatísticas apresentadas no documento, uma delas chama a atenção pelo elevado sentimento desses profissionais em relação à ameaça cibernética, como pode ser observado no gráfico da Figura 1.

Figura 1: Expectativa de profissionais do setor marítimo em relação às consequências cibernéticas no futuro próximo.



Fonte: DNV, 2023.

Essa percepção de muitos profissionais reflete o sentimento gerado pelos ataques cibernéticos ao setor marítimo ocorridos no passado que já deixaram grandes cicatrizes. Buscando planejar uma navegação adequada aos desafios vindouros, alguns desses eventos que causaram grande repercussão no setor serão analisados a seguir.

1. Tormentas passadas

Um sábio marinheiro observa o retrospecto dos mares que vai navegar em busca de conhecimentos que o ajudarão em sua rota. Da mesma forma, observar as características dos ataques cibernéticos já ocorridos contra o meio naval propicia um vislumbre do risco adiante. Nesse contexto, um dos eventos de ataques cibernéticos ao setor marítimo de maior notoriedade é, certamente, o de *ransomware*[1] ocorrido em 2017, que afligiu a gigante dinamarquesa Maersk, responsável por operar mais de 70 portos e cerca de 800 navios pelo globo.

É importante ressaltar que a Maersk não era um alvo principal, mas simplesmente se encontrava vulnerável ao *malware* utilizado nessa campanha de *ransomware*. A gênesis desse evento remonta a abril de 2017, quando um grupo *hacker* conhecido como *The Shadow Brokers* vazou um grande número de ferramentas cibernéticas provenientes da CIA e da NSA ao *site WikiLeaks* (KESSLER; SHEPARD, 2022). A mais proeminente dessas ferramentas, conhecida como *EternalBlue*, explorava uma vulnerabilidade em sistemas Windows e, embora a Microsoft tenha publicado uma correção para essa vulnerabilidade em março de 2017, grande parte dos usuários de seu sistema operacional ainda não havia aplicado essa correção quando a primeira onda de ataques ocorreu.

Em maio daquele ano, a primeira onda de ataques começou empregando o *malware* autorreplicante *WannaCry*, uma adaptação da ferramenta publicada no WikiLeaks. Em 48 horas, mais de 230.000 computadores espalhados por 150 países foram infectados, afetando diversos setores, como, por exemplo, o Sistema Nacional de Saúde da Inglaterra, que possuía, em 80% de seus computadores, o sistema operacional Windows XP, vulnerável ao *malware* (KESSLER; SHEPARD, 2022). A Microsoft, então, liberou uma correção de emergência contra o *malware* e o ataque perdeu força em alguns dias.

Um mês depois dos ataques pelo *WannaCry*, um novo *malware* entrou em circulação empregando as mesmas ferramentas. Conhecido como *NotPetya* e com autoria ligada ao grupo *hacker* russo *Cozy Bear*, esse *malware* parecia ter como alvos sites na Ucrânia, mas, devido à sua característica autorreplicante, se espalhou rapidamente pela internet e atingiu a grande rede da Maersk. O ataque obrigou a empresa a paralisar suas operações por vários dias: estima-se que tenha causado um prejuízo entre 200 e 300 milhões de dólares (FORBES, 2017).

Já no âmbito militar, quatro colisões ocorridas em 2017 – envolvendo dois *destroyers* da classe *Arleigh Burke* e dois cruzeiros de mísseis da classe *Ticonderoga* – podem fornecer *insights* das possíveis consequências de um ataque cibernético sofisticado aos meios navais. Apesar de a marinha americana negar que a causa das colisões tenha sido um ataque cibernético, o que é comum em grandes organizações que sofreram esse tipo de ataque por temerem o impacto em suas reputações, dados disponíveis em fontes abertas corroboram um diferente cenário.

Figura 2: Colisões envolvendo meios da marinha americana (*US Navy*) no Pacífico.

Fonte: USNI News, 2017.

Os quatro eventos, todos ocorridos no primeiro semestre de 2017 na região do Pacífico entre a Ásia e a Oceania, evidenciam um mesmo *modus operandi*: os quatro navios navegavam no período noturno em regiões de intenso tráfego quando, subitamente e sem nenhum comando pela equipe do passadiço, tiveram seus lemes completamente travados para um dos bordos. Como consequência dessa situação de "fora de leme" repentina, dois deles – o *USS John McCain* e o *USS Fitzgerald* – colidiram com navios mercantes. O primeiro sofreu um prejuízo material de cerca de 325 milhões de dólares, além da morte de dez de seus marinheiros. O segundo alcançou um prejuízo de 368 milhões de dólares e perdeu sete dos seus militares a bordo. Quanto aos outros dois navios, o *USS Antietam*

[1] *Ransomware*: ataque cibernético no qual um *malware* age de forma a criptografar os dados de seu hospedeiro a fim de cobrar um resgate, geralmente em criptomoedas, em troca da liberação desses dados.

colidiu com a praia sem gerar maiores danos e o *USS Lake Champlain* colidiu com um pequeno pesqueiro, sem causar perda de vidas humanas.

A Figura 2 apresenta uma visão geográfica dos quatro eventos.

No início das investigações, a marinha americana chegou a imputar acusações criminais contra os comandantes dos dois *destroyers* da classe *Arleigh Burke* por conta das vidas perdidas nas duas colisões. Contudo, com o avançar das investigações, as acusações criminais contra os comandantes foram retiradas (FOX NEWS, 2019) e o relatórios finais apontaram despreparo e erros de procedimento como as principais causas das colisões.

Contudo, outras possíveis causas sobre os quatro eventos foram debatidas, e entre elas figura a possibilidade de um ataque de cadeia de suprimentos. Quatro anos antes das colisões, em 2013, acredita-se ter sido iniciado um dos ataques cibernéticos responsáveis por um dos maiores vazamentos de dados de entidades governamentais americanas, o ataque conhecido como *The Big Hack*. Nesse ataque, *microchips* do tamanho da ponta de uma caneta foram implantados em placas de circuito integrado que eram produzidas em Taiwan e enviadas para a Califórnia, onde a empresa *SuperMicro* as empregava na construção de servidores de alta capacidade. Documentos públicos mostraram que esses servidores tiveram como clientes finais várias entidades governamentais americanas, que possivelmente receberam as placas adulteradas. Entre as organizações que receberam esses servidores estão as duas casas do congresso, a NASA e o Departamento de Defesa, inclusive com navios de guerra empregando tais servidores (BLOOMBERG, 2018).

Figura 3: Capa da Bloomberg Businessweek, 2018.

Fonte: Bloomberg, 2018.

Esses *microchips* eram capazes de receber comandos e exfiltrar dados, propiciando aos idealizadores do ataque acesso a dados sensíveis sobre os sistemas usados a bordo dos navios e, consequentemente, como explorá-los. Somente em 2015, a empresa americana *Amazon*, que também estava entre os clientes que adquiriram servidores da *SuperMicro*, percebeu um fluxo anormal de dados saindo de suas redes e, após extensa investigação interna, decidiu por desmontar seus servidores. Finalmente, os *microchips* implantados foram identificados e a empresa tornou público o ataque.

A partir das informações adquiridas por esses *microchips* e considerando que, em 2017, os quatro navios possuíam sistemas ECDIS dotados de posicionamento dinâmico que integravam o sistema de navegação e o sistema de governo, o agente por trás dos ataques reuniu as peças necessárias para findar a cadeia de ataque cibernético (*Cyber Kill Chain*). Teorias sobre o possível gatilho que acionou essa arma cibernética incluem uma junção com Guerra Eletrônica, na qual pulsos radares poderiam ser especialmente preparados para ativar um *malware* sem causar nenhuma mudança de funcionamento perceptível nos radares de navegação, de acordo com Junior e De Sá (2020). Segundo essa abordagem, o efeito dessa arma cibernética seria ativado no momento de maior vulnerabilidade dos navios, como, por exemplo, quando estivessem navegando próximo a grandes navios mercantes, mesmo que totalmente desconectados da internet ou de qualquer conexão externa no momento do ataque.

A análise em conjunto de todos esses eventos isolados, apesar de baseada em suposições, permite um vislumbre de como a capacidade cibernética pode ser empregada contra meios navais. Por meio de uma *Cyber Kill Chain* que se desenvolveu em uma janela temporal de quatro anos, o agente por trás desses ataques empregou técnicas extremamente sofisticadas, como *hardware hacking* e ataques de cadeia de suprimento, para alcançar um objetivo final.

2. Preparar para mau tempo

À medida que a evolução informacional avança, a superfície de ataque dos meios navais continuará aumentando. Destarte, é crucial que entes governamentais e privados entendam o risco atrelado e seus impactos, buscando investir no aprimoramento da cibersegurança dos sistemas navais, que geralmente são pouco maduros no que tange a essa área. Através do levantamento dos riscos e do entendimento da profundidade dessas ameaças, *stakeholders* do setor marítimo podem empregar ações práticas para robustecer suas defesas.

Após o incidente envolvendo a Maersk, a Organização Marítima Internacional (*International Maritime Organization* – IMO) tem enfatizado a importância da implementação de ações efetivas para a segurança dos sistemas a bordo dos meios navais. Em junho de

CIBERSEGURANÇA NAVAL

"O futuro do setor marítimo não mais estará apenas em mares, oceanos e águas interiores, mas também no campo de batalha invisível e transversal do quinto domínio."

2017, o Comitê de Segurança Marítima da IMO adotou a resolução MSC.428 sobre Gerenciamento do Risco Cibernético no setor. O documento tem sua gênese postulando que o Comitê reconhece a urgência de elevar a consciência situacional sobre risco cibernético e vulnerabilidades afetas a fim de fortalecer a segurança do setor (IMO, 2017). A IMO tem amplamente estimulado a adoção de estruturas (*frameworks*) de cibersegurança adequadas para o setor, como o *Guidelines on Cyber Security onboard Ships* (BIMCO, 2016) desenvolvido pelo Conselho Marítimo Internacional, em conjunto com o Conselho Mundial de Navegação e outras organizações correlatas.

Navegar por mares revoltos requer aprestamento adequado, assim como preparar esse gigante setor tão diverso para gerenciar o risco crescente e mitigar as possibilidades de um incidente cibernético a bordo ou no porto. O crescente número de vítimas de ações cibernéticas no meio naval e os eventos significativos já ocorridos têm propiciado uma mudança de postura, com uma tendência positiva de desenvolvimento da Cibersegurança Naval. As ações nesse sentido têm se concentrado em quatro pilares:

- treinamento e conscientização: uma das defesas primárias contra a ameaça cibernética é a conscientização da força de trabalho a fim de elevar sua consciência situacional cibernética. Tanto o setor privado como o militar têm buscado empreender programas de modo a garantir que seu pessoal possa reconhecer e responder perante essa ameaça;
- protocolos de segurança adequados: o emprego de ferramentas de segurança adequadas e bem configuradas é essencial. O uso de *firewall* e sistemas de detecção de intrusão, assim como a realização de auditorias regularmente estão entre as práticas mais bem difundidas;
- colaboração: o compartilhamento de Inteligência sobre as ameaças potenciais e a colaboração internacional para identificar possíveis autores têm produzido ganhos significativos. Projetos como o *Malware Information Sharing Platform* (MISP) têm contribuído para o compartilhamento de Inteligência sobre técnicas, táticas e procedimentos usados pelos *hackers*, propiciando uma consciência compartilhada das possíveis ameaças;
- desenvolvimento seguro: a construção naval e portuária precisa fomentar a ampla adoção do conceito de *Secure by Design*. É essencial que a Cibersegurança seja uma prioridade desde a concepção, com uma abordagem mais proativa a fim de implementar protocolos e sistemas com maturidade de segurança adequada a infraestruturas críticas.

A integração paulatina do setor marítimo aos sistemas digitais apresenta um paradoxo, oferecendo evolução e exposição como dois gumes de uma mesma lâmina. Conforme as ameaças cibernéticas se tornam mais sofisticadas, *stakeholders* privados e militares devem navegar nesses revoltos mares digitais com cautela e tirocínio. O futuro do setor marítimo não mais estará apenas em mares, oceanos e águas interiores, mas também no campo de batalha invisível e transversal do quinto domínio.

Referências Bibliográficas

BIMCO. **The Guidelines on Cyber Security onboard Ships**. p. 36, 2016. Disponível em: <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships>. Acesso em: 28 jan. 2024.

BLOOMBERG. **The Big Hack: how China used a tiny chip to infiltrate U.S. companies**. By Jordan Robertson and Michael Riley. Oct. 4, 2018. Disponível em: <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>. Acesso em: 4 mar. 2021.

DNV. **Maritime Cyber Priority 2023: Staying secure in an era of connectivity**. Disponível em: <https://www.dnv.com/cybersecurity/cyber-insights/maritime-cyber-priority-2023.html>. Acesso em: 28 jan. 2024.

FORBES. **NotPetya Ransomware attack cost shipping giant Maersk over $200 million**. By Lee Mathews. Aug. 16, 2017. Disponível em: <https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/?sh=6209da744f9a>. Acesso em: 25 ago. 2023.

FOX NEWS. **Navy drops charges against officers involved in fatal USS Fitzgerald collision**. By Bradford Betz. April 11, 2019. Disponível em: <https://www.foxnews.com/us/navy-drops-charges-against-officers-involved-in-fatal-uss-fitzgerald-collision-report>. Acesso em: 14 ago. 2023.

FREIRE, W. P.; et al. Blockchain-based Maritime Monitoring System. 2021 IEEE International Workshop on Metrology for the Sea: Learning to Measure Sea Health Parameters. **MetroSea 2021 – Proceedings**, p. 394-399, 2021. Disponível em: <https://ieeexplore.ieee.org/document/9611587>. Acesso em: 28 jan. 2024.

_____.Towards a Secure and Scalable Maritime Monitoring System using Blockchain and Low-Cost IoT Technology. **Sensors**, v. 22, n. 13, p. 4895, 29 jun. 2022. Disponível em: <https://www.mdpi.com/1424-8220/22/13/4895>. Acesso em: 28 jan. 2024.

INTERNATIONAL MARITIME ORGANIZATION (IMO). Resolution MSC.428(98): **Maritime Cyber Risk Management in Safety Management Systems**. v. 428, June 2017. Disponível em: <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf>. Acesso em: 28 jan. 2024.

JUNIOR, W. C. L.; DE SÁ, A. O. Triggering Cyber-electronic Attacks in Naval Radar Systems. **MetroSea 2020** – TC19 International Workshop on Metrology for the Sea, p. 12-16, 2020. Disponível em: <https://www.imeko.org/publications/tc19-Metrosea-2020/IMEKO-TC19-MetroSea-2020-03.pdf>. Acesso em: 28 jan. 2024.

KESSLER, G.; SHEPARD, S. **Maritime Cybersecurity: a Guide for Leaders and Managers**. 2nd edition. [s.l: s.n.]. 2022.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD). **Review of Maritime Transport 2022**. Chapter 1: International maritime trade and port traffic. p. 28, 2022. Disponível em: <https://unctad.org/system/files/official-document/rmt2022_en.pdf>. Acesso em: 25 ago. 2023.

U. S. NAVAL INSTITUTE NEWS (USNI NEWS). **Admiral, Captain Removed in ongoing investigations into USS John S. McCain, USS Fitzgerald Collisions; Head of Surface Forces puts in early retirement request**. By Sam Lagrone. Sep. 18, 2017. Disponível em: <https://news.usni.org/2017/09/18/admiral-captain-removed-part-investigation-uss-john-s-mccain-uss-fitzgerald-collisions-head-surface-forces-puts-early-retirement-request>. Acesso em: 14 ago. 2023.