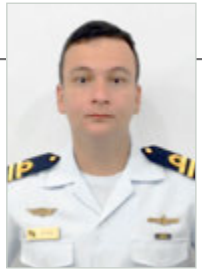
Consciência Situacional Cibernética em Operações Militares Marítimas

10



Capitão-Tenente Françoa **Taffarel** Rosário Corrêa

Graduado em Ciências Navais pela Escola Naval, com especialização em Máquinas e em Tecnologia Nuclear. Foi Oficial de Máquinas na Fragata Rademaker e Encarregado das Equipes de Proteção Cibernética e Exploração da Divisão de Guerra Cibernética do Comando Naval de Operações Especiais. É Tecnólogo em Sistemas de Computação (Universidade Federal Fluminense) e Especialista em Segurança da Informação (UNESA) e em Guerra Cibernética (Exército Brasileiro). Atualmente, é Oficial-Aluno no Centro de Coordenação de Estudos da Marinha em São Paulo (CCEMSP) e candidato a Mestre em Computação com ênfase em Guerra Cibernética (ITA – 2024). É certificado como *Professional and Experienced Penetration Tester* e coautor de três vulnerabilidades críticas em *firmwares* de dispositivos de infraestruturas críticas.

Introdução

A indústria naval, por meio de uma vasta rede composta por navios e portos, além de infraestrutura logística e administrativa, desempenha um papel crucial na dinâmica da economia global. A cada ano, aproximadamente 90% da carga mundial é transportada por essa complexa malha, que, assim como diversas outras indústrias, tem adotado níveis gradativos de automação, interconexão e monitoramento remoto. Contudo, a automação no comércio marítimo não apenas reflete a evolução tecnológica, mas também traz consigo uma vulnerabilidade cada vez maior, destacando-se como alvo primário de ataques cibernéticos. Tal vulnerabilidade é inerente à dependência de tecnologias cruciais para navegação, comunicação e logística.

Nesse cenário, a crescente utilização de operações cibernéticas em ações militares atingiu um ponto crítico de dependência, aumentando a probabilidade de interrupção ou degradação nos sistemas operacionais de um ambiente naval (KUEHL, 2009). As operações cibernéticas, ao criarem um espaço operacional para a ação militar, manifestam-se nas marinhas de maneiras diversas: desde o impacto na superioridade marítima até a perda de domínio em regiões específicas, a negação de informações sobre a posição de navios e a degradação das cadeias de suprimentos.

A progressiva dependência das informações via satélite por parte dos ativos navais ressalta a vitalidade dessas tecnologias para as redes de comunicação, garantindo uma conectividade constante aos Comandos de Força (US DOD, 2018). A capacidade de comunicar e trocar informações torna-se, assim, crucial para o sucesso operacional, proporcionando consciência situacional compartilhada e decisões de comando mais ágeis.

Durante as operações no ambiente marítimo, a comunicação via satélite em cada ativo naval requer monitoramento constante por ativos computacionais dotados da capacidade de detecção e gestão de ameaças. Esses ativos visam fornecer aos operadores a habilidade necessária para garantir que o Comandante da Força-Tarefa Marítima (FTM) tenha a Consciência Situacional Cibernética (CSC) de seus ativos navais, facilitando, assim, o processo de tomada de decisão.

Este artigo é dividido em quatro seções. Inicialmente, é efetuada uma análise de trabalhos correlatos a fim de delinear o conceito de CSC. A segunda seção destaca as características essenciais que um ativo computacional, operando no nível tático, deve possuir para contribuir efetivamente na construção da CSC. Por fim, apresenta-se um modelo de Exercício Cibernético em Operações no Mar focado no processo de tomada de decisão. A Conclusão busca integrar os pontos discutidos, ressaltando a importância da CSC no atual cenário global.

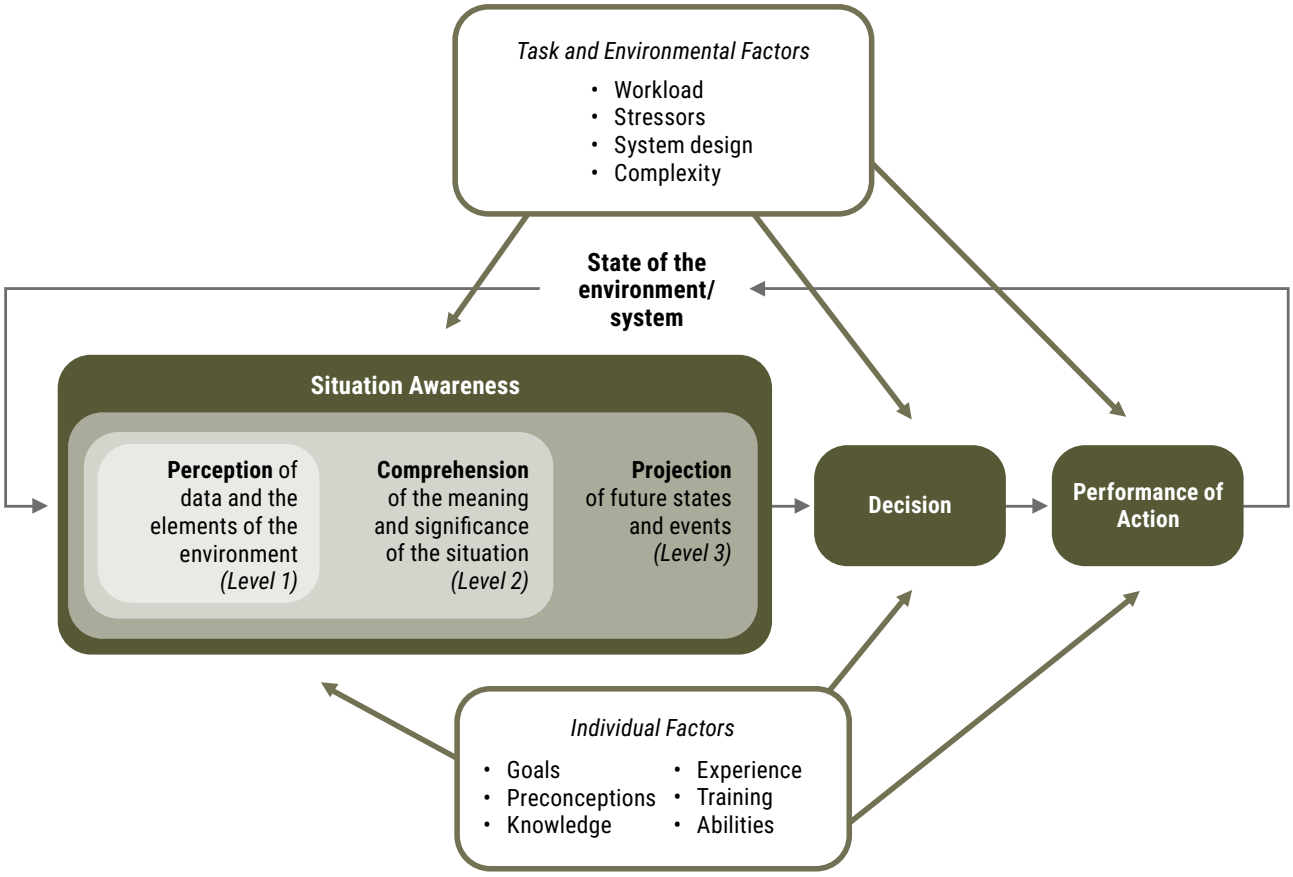
1. Definição de Consciência Situacional Cibernética

De acordo com o Glossário de Termos e Definições da OTAN, a Consciência Situacional (CS) é definida como: "O conhecimento necessário dos elementos no espaço de batalha para tomar decisões bem-informadas" (NATO, 2020b). A Consciência Situacional, integrante do processo da tomada de decisão em ambientes dinâmicos, considera objetivos, expectativas e fatores inerentes à tarefa e ao sistema utilizado.

Ao examinar a literatura existente que aborda a CS, observa-se que a maioria dos autores prefere citar ou adaptar a definição de Endsley (1995): segundo o autor, é possível construir uma CS que permita a tomada de decisões e a subsequente execução de ações, conforme o modelo delineado no Fluxograma 1, que mostra um processo de três etapas baseado em percepção dos elementos no ambiente, compreensão da situação presente e projeção sobre como o ambiente pode se apresentar em breve.

Assim, inferimos que a CSC respalda os tomadores de decisão militares ao fornecer conhecimento sobre o estado de um ambiente operacional e dos meios operacionais relevantes nele inseridos. A Doutrina Conjunta da OTAN para Operações no Ciberespaço define ciberespaço como "o domínio global que consiste em toda comunicação interconectada, tecnologia da informação e outros sistemas eletrônicos, redes e seus dados, incluindo aqueles separados ou independentes que processam, armazenam ou transmitem dados" (NATO, 2020a).

Fluxograma 1: Modelo de Consciência Situacional de Endsley.



Fonte: Endsley (1995).

Stone (2015) define a CSC como o conjunto de todos os dados sobre o estado dos sistemas operacionais que compõem o ciberespaço para uma determinada operação. Para Tyworth et al. (2012), em operações militares compostas por um ou mais meios, a CSC é o entendimento efetivo de tudo o que está associado ao domínio do ciberespaço com potencial de impactar a segurança do pessoal e do material envolvidos nas missões.

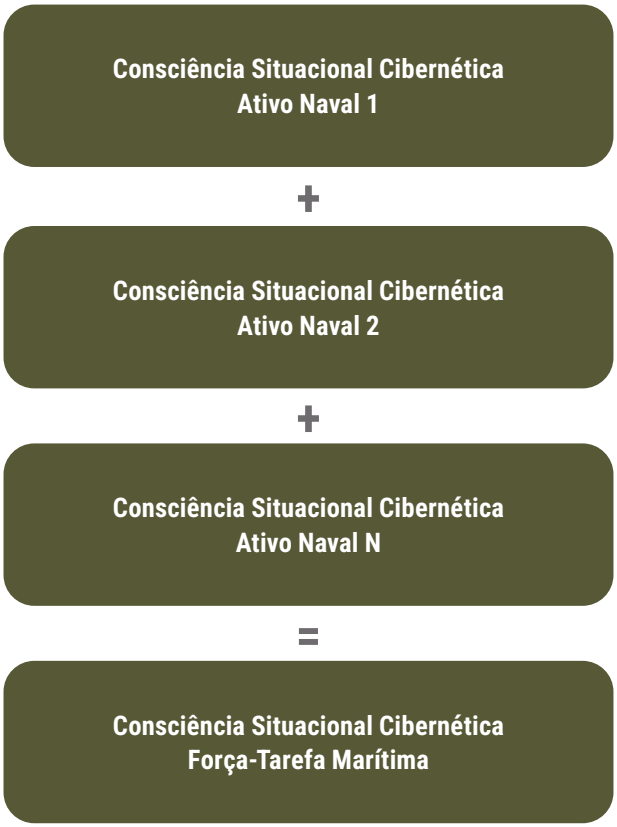
De acordo com Conti et al. (2013), uma definição de CSC em um ambiente militar é "o conhecimento atual e preditivo necessário do ambiente do qual as operações dependem — incluindo os domínios físico, virtual e humano —, bem como todos os fatores, atividades e eventos das forças amigas e adversárias em todo o espectro de conflito".

O ambiente operacional, conforme o conceito de ciberespaço da OTAN, é permeado pela comunicação de redes de computadores. A concepção adotada neste artigo, por sua vez, segue a definição de Levin et al. (2001), segundo a qual CSC é "a percepção de eventos e dados de rede, a compreensão de seu significado em termos de missão, recursos, conectividade, ameaças e vulnerabilidades, e a projeção de seu status em breve".

Assim, combinando o modelo de Endsley com a definição de Levin et al. (2001), conclui-se que a CSC é o subconjunto de toda a consciência situacional necessária para operar no e através do ciberespaço em todos os ativos navais, conforme ilustrado na Figura 1. A CSC não é um fim em si mesma, mas, fundamentada na análise constante da situação da rede de computadores,

é um meio utilizado para apoiar a tomada de decisão, permitindo que a Força-Tarefa Marítima alcance seus objetivos no domínio marítimo.

Figura 1: Consciência Situacional Cibernética da Força-Tarefa Marítima.



Fonte: O autor.

2. Um ativo digital para apoiar como construtor de Consciência Situacional Cibernética

De acordo com Kościelski et al. (2007), a Consciência Situacional Marítima (CSM) é caracterizada como o reconhecimento de eventos, atividades e circunstâncias de natureza militar e civil que ocorrem no ambiente marítimo ou a ele estão associadas. Esses elementos desempenham um papel crucial em operações e exercícios atuais e futuros da OTAN. O Ambiente Marítimo, por sua vez, abrange oceanos, mares, baías, estuários, vias navegáveis, regiões costeiras e portos.

É imperativo compilar um conjunto abrangente de informações que servirão como base para a tomada de decisões estratégicas das Forças-Tarefa Marítimas (FTM). Essa compilação envolve a coleta e a análise contínua de dados provenientes de todos os sensores e ativos computacionais disponíveis. Esse processo meticuloso requer que os dados sejam devidamente encapsulados e transmitidos de forma segura dentro dos meios navais, utilizando a rede de computadores via satélite.

Nesse contexto, com a finalidade de identificar o ativo computacional que facilita a criação da CSC, é necessário realizar ações específicas nos níveis tático e operacional. Essas atividades devem ser conduzidas pelas equipes defensivas e pelos comandantes da FTM, respectivamente. Já no nível tático, a CSC se concentra nas ameaças que exploram vulnerabilidades presentes em redes e sistemas específicos, bem como nas consequências resultantes de tais comprometimentos. As ações defensivas táticas no ciberespaço, ou através dele, visam preservar a liberdade de ação amigável no domínio cibernético, conforme indicado em NATO (2020a).

Essas ações estão em conformidade com três documentos-chave relacionados às operações defensivas no ciberespaço: a Doutrina Conjunta Aliada para Operações no Ciberespaço – AJP-3.20 (NATO, 2020a), o *Framework* de Cibersegurança do Instituto Nacional de Padrões e Tecnologia (NIST, 2018) e as Diretrizes sobre Cibersegurança a Bordo de Navios (BIMCO, 2021). As ações e estratégias defensivas incluem: identificação de ameaças cibernéticas, detecção de vulnerabilidades, avaliação de riscos, desenvolvimento de medidas de proteção e detecção, estabelecimento de planos de contingência e resposta a incidentes de segurança cibernética.

De acordo com a Doutrina Conjunta Aliada para Operações no Ciberespaço (NATO, 2020a), no plano operacional, o comandante da FTM deve levar em consideração os seguintes fatores:

- efeitos no ciberespaço: cruciais para gerar impactos táticos, operacionais e estratégicos que conduzem ao cumprimento dos objetivos militares. Esses efeitos estão intrinsecamente ligados a *softwares*, dados e protocolos, podendo também emanar de níveis cinéticos em outros domínios;
- funções conjuntas: oferecem um arcabouço que auxilia na integração e na sincronização de capacidades e atividades durante operações conjuntas;
- princípios de operação: os princípios que norteiam operações conjuntas são igualmente aplicáveis ao ciberespaço. Contudo, a interpretação desses princípios pode variar devido às características únicas desse domínio. Os princípios incluem segurança, surpresa, concentração de força, manutenção do moral e liberdade de ação.

Para otimizar os processos decisórios no nível operacional, é imperativo monitorar de forma contínua segmentos do ciberespaço a fim de identificar ameaças cibernéticas emergentes de maneira ágil e precisa. Nesse sentido, faz-se necessária a implementação de uma ferramenta eficaz que não apenas operacionalize todas as informações pertinentes, mas também ofereça uma

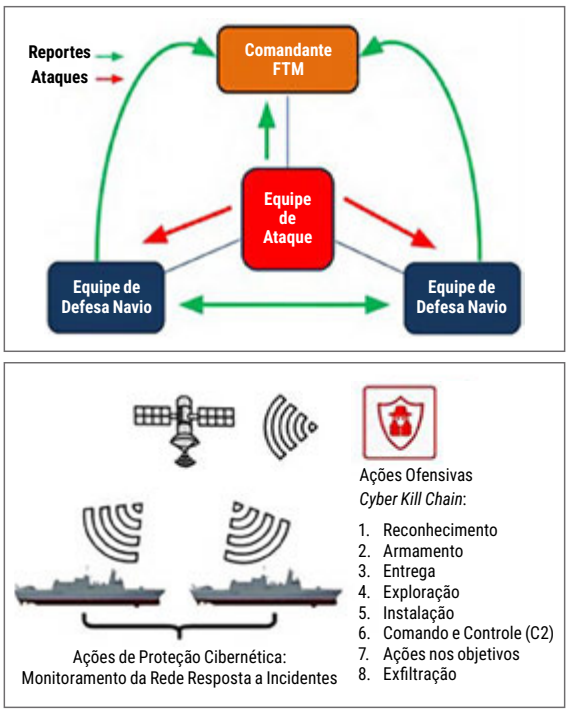
análise profunda das condições presentes e futuras no ciberespaço. Essa ferramenta, idealmente instalada em cada ativo naval pertencente à FTM, deve possuir as seguintes capacidades:

- visibilidade em tempo real: proporcionar uma visão clara e atualizada das ameaças existentes em todo o domínio do ciberespaço;
- identificação rápida de ameaças: reconhecer ameaças de forma rápida e eficiente;
- análise de registros: possuir funcionalidades que permitam a pesquisa e a análise de registros, facilitando a investigação de incidentes potenciais;
- redução do tempo de resposta: minimizar o tempo necessário para responder a incidentes e ameaças, aumentando a eficácia das medidas de proteção implementadas.

3. Conduzindo um exercício cibernético em operações reais no mar

Este artigo propõe a realização de um Exercício Cibernético em Operações Reais no Mar com o propósito de avaliar a eficácia do aumento da Consciência Situacional Cibernética (CSC) no aprimoramento do processo decisório. O exercício sugerido envolve duas equipes operando em posições opostas no ciberespaço da Força-Tarefa Marítima (FTM): uma equipe encarregada da defesa do ciberespaço, e a outra responsável pelo papel de atacante.

Figura 2: Exercícios Cibernéticos via Comunicações por Satélite.



Fonte: O autor.

Conforme ilustrado na Figura 2, ambas as equipes devem reportar ao comandante da FTM os efeitos resultantes de suas ações no ciberespaço da entidade. Essa avaliação contínua (*feedback*) visa fornecer conhecimentos (*insights*) valiosos sobre o impacto das operações cibernéticas no ambiente marítimo.

Segundo Domingo et al. (2021), para aprimorar o processo de tomada de decisão por meio da CSC, o comandante da FTM deve ser capaz de responder a algumas perguntas essenciais, como:

- que operações estão sendo conduzidas no ciberespaço;
- qual o impacto dos efeitos do ciberespaço na missão em curso;
- quantas tecnologias operacionais foram incapacitadas em decorrência do incidente cibernético;
- após o incidente cibernético, qual o nível de comprometimento da infraestrutura de informação dos ativos navais envolvidos na missão.

Essas perguntas são cruciais para avaliar a extensão do dano causado por incidentes cibernéticos e para compreender como tais incidentes podem afetar as operações em curso. Responder a essas perguntas de maneira precisa e tempestiva é fundamental para a implementação de estratégias de resposta eficazes e para a manutenção da integridade das operações marítimas. As ações propostas devem ser executadas na mesma banda de comunicação via satélite utilizada para navegação. Cada equipe de defesa a bordo dos navios tem a responsabilidade de coletar, analisar e identificar dados de rede, além de monitorar ativamente a presença de incidentes cibernéticos críticos que possam afetar a Força-Tarefa Marítima (FTM).

Esse processo contínuo de vigilância e análise fornece ao comandante uma Consciência Situacional Cibernética robusta e atualizada que é fundamental para a tomada de decisões abrangentes, confiáveis e tempestivas visando ao cumprimento bem-sucedido da missão designada.

Na outra vertente, a equipe encarregada das ações ofensivas deve adotar estratégias proativas, valendo-se, por exemplo, da metodologia *Cyber Kill Chain*, desenvolvida por especialistas da Lockheed Martin. De acordo com Hutchins et al. (2011), esse modelo proporciona um *framework* estruturado para a compreensão e a prevenção de ciberataques, como pode ser visualizado na Figura 2. A aplicação da *Cyber Kill Chain* capacita a equipe ofensiva a executar ações coordenadas e estratégicas em todo o ciberespaço da Força-Tarefa Marítima, identificando e explorando vulnerabilidades de maneira eficaz e sistemática.

Uma vez que os exercícios propostos serão realizados em operações reais no mar, direcionadas ao ciberespaço da Força-Tarefa Marítima, é imperativo estabelecer métricas claras e verificáveis para avaliar o desempenho de cada equipe envolvida. Essas métricas servirão como indicadores-chave de desempenho para as ações executadas pelas equipes, fornecendo uma base objetiva para análise e avaliação.

Para a equipe de defesa dos navios, a avaliação pode fundamentar-se no número de incidentes cibernéticos identificados, quantificando a capacidade da equipe de detectar ameaças ativas no ciberespaço. Além disso, o número de incidentes cibernéticos bloqueados mensura a eficácia das estratégias de defesa implementadas para neutralizar ou mitigar ameaças. A comunicação eficiente e tempestiva de eventos críticos ao comando superior também é vital; assim, o número de incidentes reportados ao Comandante da FTM se configura como um indicador relevante para a tomada de decisões informadas e rápidas.

A equipe de ataque, por outro lado, pode ser avaliada por sua proficiência em identificar pontos fracos ou falhas nos sistemas de Tecnologia da Informação (TI) e Tecnologia Operacional (TO) embarcados nos ativos navais, sendo o resultado indicado pelo número de vulnerabilidades descobertas. O impacto efetivo das ações ofensivas também constitui um critério crucial de avaliação, sendo quantificado pelo grau de interrupção ou comprometimento das funções e sistemas críticos a bordo dos navios, ou seja, pelo número de degradações de TI/TO.

Essas métricas proporcionam uma visão clara e quantitativa do desempenho de cada equipe, facilitando a avaliação objetiva de suas competências e sua eficácia durante os exercícios. Além disso, oferecem *insights* valiosos para o aprimoramento contínuo das estratégias de defesa e ataque no ciberespaço marítimo.

Conclusão

Os ataques cibernéticos têm se intensificado no Domínio Marítimo, elevando a segurança cibernética a uma preocupação global crescente. No cenário marítimo militar, no qual as operações podem ser alvos desses ataques, é crucial que os comandantes das Forças-Tarefa Marítimas estejam aptos a integrar a Consciência Situacional Cibernética em suas estratégias e processos decisórios.

O desfecho de conflitos militares futuros será fortemente influenciado pela capacidade de cada lado para coletar, processar e disseminar informações de maneira eficaz e ágil, possibilitando decisões mais acertadas e rápidas do que as do adversário. Nesse contexto, a CSC emerge como ferramenta vital para os Comandantes da FTM, auxiliando-os a navegar com segurança e eficácia diante dos desafios impostos pelos ataques cibernéticos.

Portanto, a segurança de rede não é apenas um desafio, mas também uma responsabilidade compartilhada globalmente. Nenhuma nação pode se dar ao luxo de permanecer alheia, focando exclusivamente em sua própria segurança cibernética. A responsabilidade de garantir uma rede segura e resiliente deve ser compartilhada por toda a comunidade internacional.

Tendo em vista a realização de trabalhos futuros, pretende-se conduzir o Exercício Cibernético e quantificar os riscos e os impactos gerados pelas equipes ofensivas ao Domínio Marítimo durante as operações militares, o que fornecerá *insights* valiosos para fortalecer as estratégias de defesa e resposta a incidentes cibernéticos no ambiente marítimo.

Referências Bibliográficas

BALTIC AND INTERNATIONAL MARITIME COUNCIL (BIMCO). **The Guidelines on Cyber Security Onboard Ships**. Version 4.0, 2021.

CONTI, G.; NELSON, J.; RAYMOND, D. Towards a cyber common operating picture. In: PODINS, K.; STINISSEN, J.; MAYBAUM, M. (Eds.). **International Conference on Cyber Conflict**. Tallinn: NATO CCD COE Publications, 2013. p. 1-17.

DOMINGO, Alberto; et al. Enabling NATO Cyberspace Operations by Building Comprehensive Cyberspace Situational Awareness. In: LOPEZ JR, Juan; PERUMALLA, Kalyan; SIRAJ, Ambareen (Eds.). **ICCWS 2021: Proceedings of the 16th International Conference on Cyber Warfare and Security**. [S.l.: s.n.], 2021. p. 509-518.

ENDSLEY, M. R. Toward a theory of situation awareness in dynamic systems. Human Factors. **The Journal of the Human Factors and Ergonomics Society**, v. 37, n. 1, p. 32-64, 1995.

HUTCHINS, Eric; CLOPPERT, Michael; AMIN, Rohan. **Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains**. 2011.

KOŚCIELSKI, M.; MILER, R.K.; ZIELIŃSKI, M. Maritime Situational Awareness (MSA). **Zeszyty Naukowe Akademii Marynarki Wojennej**, v. 48, n. 4 (171), p. 79–88, 2007.

KUEHL, D.T. From cyberspace to cyberpower: Defining the problem. In: KRAMER, F. D.; WENTZ, L.K.; STARR, S. H. (Ed.). **Cyberpower and National Security**. Dulles, VA: Potomac Books, Inc., 2009.

LEVIN, D.; TENNEY, Y.; HENRI, H. Issues in human interaction for cyber command and control. In: DARPA Information Survivability Conference, 1., 2001. **Anais** [...]. [S.l.: s.n.], 2001. p. 141–151.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Framework for Improving Critical Infrastructure Cybersecurity.** Version 1.1. NIST Cybersecurity Framework, April 2018. Disponível em: <https://doi.org/10.6028/NIST.CSWP.04162018>. Acesso em: 30 jan. 2024.

NORTH ATLANTIC TREATY ORGANIZATION (NATO). NATO Standardization Office (NSO). **Allied Joint Doctrine for Cyberspace Operations**. AJP-3.20, Edition A, Version 1, 2020a.

_____·_____· **NATO Glossary of Terms and Definitions** (English and French): AAP-06. Page 119. Edition 2020b.

STONE, Steve. Data to Decisions for Cyberspace Operations. **Military Cyber Affairs**, v. 1, n. 1, Article 6, 2015.

TYWORTH, M.; GIACOBE, N. A.; MANCUSO, V. M. Cyber situation awareness as distributed socio-cognitive work. In: **Cyber Sensing - Proceedings of SPIE**, v. 8404, 2012.

UNITED STATES DEPARTMENT OF DEFENSE (US DOD). Joint Chiefs of Staff. Joint Publication 3-32: **Joint Maritime Operations**. June 8, 2018. Disponível em: <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_32ch1.pdf>. Acesso em: 30 jan. 2024.