OPINFO E GUERRA DA INFORMAÇÃO
NA GUERRA NAVAL

Capitão de Corveta **ANTONIO** FELIPE DO NASCIMENTO E SOUSA
Encarregado do Grupo de Ensino à Distância – CAAML
Aperfeiçoado em Comunicações

FONTE: Marinha do Brasil / Getty Images
Composição Fotográfica: 1ºSG Severiano

INTRODUÇÃO

Ao longo da evolução humana, a capacidade de obter, compreender, controlar e fazer uso efetivo da informação sempre foi um fator decisivo para o êxito nas mais diversas áreas de conhecimento e atividades, incluindo ações relacionadas ao poder militar. A crescente velocidade na produção e no fluxo de informações relacionadas à revolução tecnológica e à transformação digital potencializou as diferenças entre aqueles que exploram adequadamente a dimensão informacional e os que ainda a consideram mera fonte de subsídios para ações na dimensão física.

Essa realidade tem impulsionado esforços de importantes atores internacionais no sentido de desenvolver e consolidar doutrinas, além de sistematizar táticas, técnicas e procedimentos relacionados ao uso da informação em operações militares. Entretanto, tais atores enfrentam desafios de diferentes naturezas e origens, como a velocidade de surgimento de novos conceitos e tecnologias, o tempo necessário para capacitação e aperfeiçoamento do pessoal e alguma resistência às mudanças de paradigma necessárias.

Neste artigo, serão apresentados alguns dos aspectos em evidência atualmente, sem a pretensão de esgotar o assunto ou apresentar caminhos a serem seguidos, mas com o intuito de ampliar o alcance e o interesse nas discussões afetas à Guerra da Informação (*Information Warfare – IW*), em especial no contexto dos meios navais de superfície. Ressalta-se, entretanto, que, considerando a disponibilidade de material sobre o tema e o enquadramento geopolítico e estratégico do país, as discussões apresentadas estão inseridas em um contexto ocidental específico, portanto eventuais extrapolações ou generalizações devem ser evitadas.

EVOLUÇÃO DE TERMOS E CONCEITOS BÁSICOS

O uso da dimensão informacional para fins militares definitivamente não é um tema recente, já que, em diversas passagens históricas, a dissimulação apresenta-se como importante (e frequentemente decisiva) ferramenta para o sucesso de uma operação militar. Este emprego manteve, essencialmente, seu propósito principal de comprometer o processo decisório do inimigo e garantir a integridade da própria sistemática de Comando e Controle (C2), porém foi incorporando novos métodos e conceitos ao longo do tempo.

Os conhecimentos obtidos e o desenvolvimento de tecnologias disruptivas durante a Segunda Guerra Mundial e conflitos posteriores, com destaque para o período da Guerra

Fria, aceleraram e intensificaram esses incrementos. Nesse ponto, cabe breve pausa na linha cronológica para apresentar resumidamente o conceito atual de Capacidade Relacionada a Informação (CRI) que se refere a "qualquer atividade ou ferramenta capaz de afetar a informação em qualquer uma das três perspectivas da dimensão informacional,[1] podendo incluir ataques físicos, ações cinéticas e não cinéticas".

Assim, ao Despistamento ou Dissimulação[2] foram se somando novas capacidades, como as relacionadas à Guerra Eletrônica, à Segurança das Informações e à Destruição Física, contempladas no conceito estadunidense de Guerra de Comando e Controle (*Command and Control Warfare*), do final da década de 1980.

Ao longo da década de 1990, a ampliação da cobertura dos conflitos em todo o mundo por parte da mídia e o sucesso em intensiva campanha de Operações Psicológicas por parte de forças da Coalizão, durante a 1ª Guerra do Golfo, amplificaram a percepção da importância das ações no campo informacional.

Assim, em 1996, o Departamento de Defesa dos EUA passou a utilizar o termo Operações de Informação (OpInfo), que incorpora implicitamente o fato de determinadas ações serem realizadas mesmo em tempos de paz, visando formatar a dimensão informacional de forma favorável. Modernamente, esta expressão é bastante utilizada pelos países pelo seu caráter mais amplo.

A terminologia "Guerra da Informação" é adotada pela MB quando se refere a ações durante o período de crise e conflito, porém outros países, eventualmente, distinguem doutrinariamente o emprego desses termos de acordo com outros critérios. Os EUA, por exemplo, diferenciam-nos principalmente pelo nível de condução da guerra.

Na virada do século, a popularização da Internet, o surgimento e o crescimento das mídias sociais e a crescente dependência da Tecnologia da Informação e Comunicações (TIC) trouxeram novos elementos para o contexto das OpInfo, não somente com a intensa evolução das capacidades já existentes, mas também com o desenvolvimento de ações em novo espaço: o cibernético. As possibilidades dessa nova fronteira evidenciaram sua progressiva relevância, levando ao reconhecimento pela Organização do Tratado do Atlântico Norte (Otan), em 2016, do Espaço Cibernético (ECiber) como um novo domínio operacional.

AS OPINFO E A GUERRA NO MAR

No contexto naval, essa recente evolução também foi foco de atenção das forças e, no início da década de 1980, diversos conceitos relacionados, com destaque para a Guerra Eletrônica (e Acústica) e Segurança das Comunicações, permeavam os procedimentos estabelecidos para os ambientes tradicionais da guerra no mar. Nessa época, por exemplo, já havia a previsão na estrutura CWC (*Composite Warfare Commander*) da figura do Coordenador de Guerra Eletrônica (*Electronic Warfare Coordinator*) e de suas tarefas, além da responsabilidade de coordenação das ações de Guerra Acústica, normalmente atribuída ao Comandante da Guerra Antissubmarino (*Antisubmarine Warfare Commander*).

Desde então, algumas atualizações incrementais em conceitos e procedimentos foram realizadas, normalmente acompanhando os avanços dos recursos e a ampliação do uso de determinadas ferramentas, porém discussões sobre a necessidade de mudanças mais significativas surgiram com o advento das ações de Guerra Cibernética (GC), suas aplicações e possíveis efeitos no contexto das forças navais.

Assim, desde 2009, a *US Navy* vem conduzindo profundas transformações, visando adequar-se a essa nova realidade. Em relação à doutrina, amplamente revisada e com criação de novas diretrizes, os principais destaques foram:

- a definição estratégica, em 2014, dos três pilares da IW[3]: Consciência Situacional do Teatro de Operações; Comando e Controle confiável; e "Fogos Integrados";[3] e
- a designação das áreas de atuação da IW, integrando informações, redes de comunicações, inteligência, criptologia, o espaço cibernético, guerra eletrônica, meteorologia e oceanografia e o domínio espacial.

No tocante à organização, foram marcantes:

- reorganização, em 2009, da estrutura do OPNAV (*The Office of the Chief of Naval Operations*), com a criação do "OPNAV N2/N6", que combinava as funções de inteligência (N2) e de comunicações (N6),[4] além de elementos relacionados a informação de outros setores,[5] e passou a ser o representante responsável pelo Domínio da Informação;[6]
- criação, ainda em 2009, do *Information Dominance Corps* (IDC), renomeado (em 2016) como *Information Warfare Community* (IWC);
- (re)ativação da *U.S. Tenth Fleet* como *U.S. Fleet Cyber Command*, em 2010, com tarefas diretamente relacionadas ao uso do ciberespaço de interesse da *US Navy*, além de negar tal uso pelos adversários; e
- criação do Comando *Navy Information Forces* (Navifor) em 2014, originalmente sob a denominação *Information Dominance Forces Command* (até a mudança de IDC para IWC), responsável principalmente por desenvolver e manter a capacidade de pronto emprego de forças de IW a serem empregadas pela *US Navy* e em operações conjuntas.

No nível tático, merece destaque a atualização da estrutura CWC, com a inclusão do Comandante da Guerra da Informação (*IW Commander – IWC*[7]), a quem cabe moldar e avaliar o ambiente informacional, alcançar e manter a superioridade da informação, desenvolver e executar os planos de OpInfo em apoio aos objetivos do OCT/CWC, enquanto apoia os outros comandantes de guerra. Além disso, foi relevante a padronização da subordinação ao IWC das atividades de inteligência (atribuídas ao N2) também neste nível (e não somente no nível operacional).

Evidentemente, é imprescindível a formação e contínua capacitação de recursos humanos, além da captação de pessoal especializado, de modo a consolidar uma massa crítica para implementar, conduzir e acompanhar todos esses desenvolvimentos tecnológicos, doutrinários e organizacionais. Deste modo, a *IW Community*, gerenciada pelo *OPNAV N2/N6*, é composta por Oficiais e Praças agrupados por áreas de conhecimento e atuação, normalmente apresentadas da seguinte maneira:

- Comunicações[8] – possuem atribuições atinentes à operação segura e integrada dos sistemas e redes de comunicações e de combate, permeando todos os ambientes de guerra e domínios, com ênfase na gestão da informação e garantia do C2;
- Inteligência – conduzem operações de inteligência para desenvolver um conhecimento aprofundado sobre as capacidades, intenções e atividades do inimigo; e fornecem, oportunamente, avaliações preditivas relevantes de variadas fontes para apoio a decisão no nível tático, no operacional e no estratégico;
- Criptologia – atuam na criptologia, no espaço, na inteligência de sinais, nas ações de Guerra Cibernética e de Guerra Eletrônica para garantir a liberdade de ação (aspecto defensivo), além de alcançar objetivos militares (aspecto ofensivo) por meio do espectro eletromagnético, do ECiber e espaço, ou no contexto destes;
- Guerra Cibernética – atuam especificamente nas ações de Guerra Cibernética com aplicações mais técnicas, sendo necessário especialização e treinamento em áreas de conhecimento relacionadas a tecnologias disruptivas e desenvolvimento de capacidades no ECiber; e
- Oceanografia e Meteorologia – visam coletar, processar e explorar informações ambientais (oceanográficas, meteorológicas, hidrográficas, de tempo preciso e astrométricas) com impactos nas operações militares, de modo a garantir segurança e subsidiar decisões.

HÁ CONTROVÉRSIAS...

Como esperado, as mudanças implementadas não ficaram imunes a questionamentos e divergências, seja por parte daqueles que as consideram insuficientes ou conservadoras demais em face das necessidades impostas ou pelos que acreditam que carecem de maior análise e gradatividade.

FONTE: www.marines.mil

Entre as principais discussões em curso sobre o tema, estão:

- **IW como ambiente específico na guerra naval** – conforme abordado, os assuntos de IW têm interseções com os ambientes tradicionais e, possivelmente por esse motivo, há quem afirme que a IW serviria apenas de suporte às demais guerras e que as premissas para algumas das mudanças implementadas seriam baseadas em analogias falsas. Sob esse prisma, as referidas alterações, em especial no nível tático, atenderiam apenas a demandas burocráticas e não demonstrariam benefício efetivo. Contudo, o entendimento de que as possibilidades da IW estão muito além de simples apoio tem crescido e sua relevância no alcance de objetivos tem sido usada como fundamento para a defesa da nova configuração da estrutura CWC.

- **Operação do IWC embarcado em um *Carrier Strike Group* (CSG) ou de Centros de Operações (*Maritime Operations Centers*, MOC)** – a segunda opção foi testada a partir de 2021, com o objetivo de permitir o acesso do IWC a informações táticas de múltiplas plataformas e sistemas no contexto de uma operação combinada, além de aproximá-lo das decisões do nível operacional. Entretanto, há considerações a respeito do afastamento do ambiente no qual o CSG está operando e seus eventuais impactos na eficiência na obtenção de informações e assessoramento remoto aos envolvidos.

- **Delimitação e consolidação das CRI** – apesar da definição doutrinária das áreas de atuação da IW, na prática, ainda há divergências de interpretação, seja por interseções entre as CRI em si ou por suas relações com outras áreas de conhecimento. Os exemplos mais comuns são o cruzamento entre as ações da Guerra Cibernética e da Eletrônica, no tocante

ao uso do espectro eletromagnético para tráfego de dados em redes específicas; e o posicionamento da inteligência sob a esfera da IW, considerando, especialmente, as diversas acepções sobre a "Inteligência" e seu emprego no contexto militar (como função, atividade no sentido amplo ou estrito, ou operação). A esse respeito, a avaliação é que a contínua capacitação e o desenvolvimento da mentalidade permitirão melhor estabelecimento dos conceitos correlatos.

- **OpInfo em cada nível de condução da guerra** – a melhor definição das possibilidades de emprego e a avaliação da necessidade de descentralização permeiam vários debates, como, por exemplo, quanto ao emprego de ações de Guerra Cibernética de exploração e ataque (e não somente de proteção) no nível tático, considerando a possibilidade de acesso a redes locais do inimigo eventualmente inacessíveis por elementos que conduzem a GC no nível estratégico ou no operacional. Os principais contrapontos para o caso deste exemplo são a possibilidade de danos colaterais indesejados, ocasionando escalada da crise ou conflito, e o risco de tornar públicas ferramentas importantes, o que permitiria o desenvolvimento de proteção contra estas, mas também se considera o fato de que objetivos de oportunidade neste contexto são raros.

- **Distribuição de pessoal da IWC pelos meios** – de certa forma, relacionada à descentralização citada acima, mas com reforço às necessidades de cada unidade, em contraposição à visão prevalecente atual de concentrar o pessoal nas Unidades de Maior Valor (*High-Value Units* – HVU) e/ou no Capitânia, especialmente considerando a possibilidade de operação em ambiente de C2 degradado ou negado (*Command and Control Degraded or Denied Environment* – C2D2E). Naturalmente, a disponibilidade de pessoal qualificado é fator condicionante para essa eventual desconcentração, mas a priorização do guarnecimento nas HVU representa a assunção de riscos considerados desconfortáveis nos navios de menor porte.

CONSIDERAÇÕES FINAIS

Mesmo considerando o contexto específico no qual esse artigo se baseou, as transformações implementadas pelos EUA em um período relativamente pequeno evidenciam a prioridade que aquela potência mundial tem dado ao Domínio Informacional, pelos motivos já apresentados.

Os países que buscam alcançar (ou manter) papel relevante na conjuntura global, devem compreender e participar dessa evolução, adequando-a às suas realidades e a seus interesses estratégicos, com ênfase no desenvolvimento de capacidades, profundamente relacionado com a formação da massa crítica preparada para conduzir as OpInfo e/ou a Guerra da Informação.

Notas

1- Física, cognitiva ou lógica.

2- Despistamento é o termo previsto na Doutrina Militar Naval, enquanto o Exército Brasileiro emprega Dissimulação.

3- Do original: Battlespace Awareness, Assured Comand and Control, and Integrated Fires. "Fogos Integrados" (tradução do autor) é conceito que contempla as coordenações necessárias para manter a iniciativa das ações, por meio do emprego de armamentos cinéticos e não cinéticos da própria força, bem como para limitar a liberdade de manobra e ação por parte do inimigo.

4- *Office of the Director of Naval Intelligence* (N2) e *Office of the Deputy Chief of Naval Operations* (DCNO) *for Communication Networks* (N6).

5- OpInfo e Operações Cibernéticas (N39) e programas e recursos de sistemas autônomos (originalmente da estrutura do N8).

6- Tradução livre de *Information Dominance*, definido como a superioridade na geração, manipulação e emprego da informação suficiente para proporcionar aos seus detentores o domínio militar.

7- Neste artigo, quando necessário será especificado se Community ou Commander.

8- Originalmente "*Information Professionals*", mas a análise de sua atuação levou a tradução "Comunicações".

.

Referências

BUTERA, Tony. Navy information warfare needs more resources – and command at sea. **Proceedings**, Anápolis, MA, v. 145, n. 1, 2019. Disponível em: https://www.usni.org/magazines/proceedings/2019/january/navy-information-warfare-needs-more-resources-and-command-sea. Acesso em: 13 mar. 2023.

DEPARTMENT OF THE NAVY (Estados Unidos). **Intelligence support to naval operations NWP 2-01**. Norfolk: Department of the Navy, 2010. Disponível em: https://info.publicintelligence.net/USNavy-IntelSupportNavalOps.pdf. Acesso em: 4 abr. 2023.

EHRLANDER, Lars; STOREY, Brad. Intelligence officer under information warfare – a bolstered role. **Proceedings**, Anápolis, MA, v. 145, n. 8, 2019. Disponível em: https://www.usni.org/magazines/proceedings/2019/august/intelligence-officer-under-information-warfare-bolstered-role. Acesso em: 13 mar. 2023.

HASSELTINE, George. Commanders need cyber weapons for maneuver warfare. **Proceedings**, Anápolis, MA, v. 145, n. 4, 2019. Disponível em: https://www.usni.org/magazines/proceedings/2019/april/commanders-need-cyber-weapons-maneuver-warfare. Acesso em: 20 mar. 2023.

MARINHA DO BRASIL. Estado-Maior da Armada. **Doutrina de operações de informação**: EMA-335. Brasília, DF: Estado-Maior da Armada, 2018.

MINOR, John. The navy must decentralize information warfare. **Proceedings**, Anápolis, MA, jan. 2022. Disponível em: https://www.usni.org/magazines/proceedings/2022/january/navy-must-decentralize-information-warfare. Acesso em: 20 mar. 2023.

PALMIERI, Margaret. Integrated fires. **Proceedings**, Anápolis, MA, v. 140, n. 7, 2014. Disponível em: https://www.usni.org/magazines/proceedings/2014/july/integrated-fires. Acesso em: 4 abr. 2023.

SHELBOURNE, Mallory. Navy to experiment with information warfare commanders operating from maritime operations centers. **USNI News**, [*S. l.*], 22 abr. 2021. Disponível em: https://news.usni.org/2021/04/22/navy-to-experiment-with-information-warfare-commanders-operating-from-maritime-operations-centers. Acesso em: 20 mar. 2023.

STEPHENSON, Henry. Navy information warfare: a decade of indulging a false analogy. **Proceedings**, Anápolis, MA, v. 145, n. 1, 2019. Disponível em: https://www.usni.org/magazines/proceedings/2019/january/navy-information-warfare-decade-indulging-false-analogy. Acesso em: 13 mar. 2023.

SUMME, Jack. Navy's new strategy and organization for information dominance. **CHIPS**, [*S. l.*], 2010. Disponível em: https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=2557. Acesso em: 4 abr. 2023.

THEOHARY, Catherine. **Defense primer**: information operations. CRS. [2022]. Disponível em: https://crsreports.congress.gov/product/pdf/IF/IF10771. Acesso em: 4 abr. 2023

UNITED STATES NAVAL ACADEMY. **Information warfare commander and cryptologic resource coordinator info sheet**. Anápolis, MA: USNA, [20--?] Disponível em: https://usna.edu/InformationWarfare/_files/documents/service_assignment/Information_Warfare_Commander_and_Cryptologic_Resource_Coordinator_Info_Sheet.pdf. Acesso em: 20 mar. 2023.