O NOVO PARADIGMA DE COMANDO E CONTROLE NAS OPERAÇÕES CONJUNTAS: Um desafio à implementação do Sistema de Gerenciamento da Amazônia Azul (SisGAAz)

Roger Pinesso da Silva [1]

RESUMO

A era da informação, em que vivemos, permite que enormes massas de dados sejam disponibilizadas, dificultando o trabalho dos decisores e suas equipes. Hoje, temos as Operações de informação que podem manipular as atitudes de amigos e oponentes. Os conceitos de Guerra Centrada em Redes favorecem a tomada de consciência da situação em localidades remotas com informações oportunas, precisas e relevantes. Informações essas, que

1 Escola de Guerra Naval (EGN), Rio de Janeiro, RJ, Brasil. E-mail: pinesso@egn.mar.mil.br, endereço: Escola de Guerra Naval, Avenida Pasteur 480, Urca, Rio de janeiro, RJ, Brasil, CEP: 22.290-240. Instrutor de Planejamento Militar e Comando e Controle da Escola de Guerra Naval e, atualmente, Encarregado da Área de Estudos I – Operações Navais e Jogos de Guerra.

filtradas e avaliadas por pessoal treinado, são empregadas em indicadores de desempenho, os quais condicionam a condução de operações militares. Além disso, há a ameaça da Guerra Cibernética que pode interromper, confundir ou mesmo furtar o fluxo de informações indispensável ao Comando e Controle (C2). Outra questão atual é a necessária garantia de C2 ágil tanto para a vigilância quanto para a aplicação da força. Tudo isso aponta para soluções de C2 passíveis de emprego prático no SisGAAz, um dos desafios fundamentais da Marinha do Brasil.
Palavras-chave: Informação. Redes. Operações. Comando. Controle.

THE NEW PARADIGM OF COMMAND AND CONTROL IN JOINT OPERATIONS: a challenge to the implementation of the Blue Amazon Management System (SisGAAz)

ABSTRACT

The information age, in which we live, allows huge amounts of available data, hampering the work of decision makers and their teams. Today, we have the information operations that can manipulate the attitudes of friends and opponents. The Network Centric Warfare concepts favor awareness of the situation in remote locations with timely, accurate and relevant information. Such information filtered and evaluated by trained personnel is employed on performance indicators, which determine the conduct of military operations. In addition, there is the threat of Cyber War, which can break, confuse or even steal the flow of vital information to the Command and Control (C2). Another current issue is the necessary guarantee of agile C2 for surveillance,

as well as for force employment. All this points out to practical C2 solutions employment in SisGAAz, one of Brazilian Navy key challenges.
Keywords: Information. Networks. Operations. Command. Control.

INTRODUÇÃO

O Comando e Controle (C2) aplica-se naturalmente às atividades militares. Comandar e Controlar são atividades do cotidiano dos líderes, seja na paz ou no conflito. Eles buscam garantir que seus subordinados assumam atitudes e tomem ações necessárias ao cumprimento da missão recebida. Pode-se fazer uma analogia entre C2 e o sistema nervoso humano. O cérebro corresponde ao Comandante e seu Estado-maior; os nervos às redes; os sentidos aos sensores; e os músculos dos membros às tropas, blindados, aeronaves, navios e comunicação social no âmbito de uma força conjunta. Há um ciclo de informações que vai dos sentidos e músculos ao cérebro e retornam do cérebro aos músculos e sentidos para gerar movimento. Esse mesmo ciclo se verifica entre o Comandante e seus comandados para gerar ações nas operações e campanhas.

A exemplo do sistema nervoso, a complexidade do C2 nas campanhas militares da atualidade é grande:

> Imagine-se numa posição comparável à encarada pelo General Norman Schwarzkopf na Guerra contra o Iraque. Você está no comando e é responsável pelas forças de coalizão de dezoito ou mais nações que enfrentam as forças de Saddan Hussein. Aquelas forças falam diferentes línguas, lutam com diferentes armamentos e táticas, e em alguns casos guardam mútuas e antigas inimizades (COAKLEY, 1991, p. 3).

Tal emaranhado de forças multinacionais é uma realidade, seja em conflitos abertos, seja em operações de paz sob a égide da ONU, como são os casos da MINUSTAH no Haiti e da Força-Tarefa Marítima da UNIFIL-FTM no Líbano, em que o Brasil atua como nação-líder.

Mas, o desafio do C2 vai além das dificuldades de condução de uma força multinacional. Vivemos na era da informação, em que a facilidade de comunicação faz com que uma enorme massa de dados seja disponibilizada a muitos, o que aumenta bastante o trabalho dos decisores

perante o andamento das operações e a mídia. Operações de Informação[2] manipulam as atitudes de amigos e oponentes em favor de interesses específicos. As redes de dados permitem a tomada de consciência da situação em localidades remotas, de maneira compartilhada e simultânea, de modo a incrementar a oportunidade, a precisão e a relevância das informações disponibilizadas aos meios e aos decisores. Essas informações, filtradas e avaliadas por pessoal treinado, são empregadas em indicadores de desempenho que condicionam a condução de campanhas e grandes operações. Além disso, há a ameaça da Guerra Cibernética que pode interromper, confundir ou furtar o fluxo de informações indispensável e, até mesmo, causar danos materiais às nossas infraestruturas de C2. Outra questão é a necessária garantia de C2 suficientemente ágil e adaptado tanto para a vigilância quanto para a aplicação da força.

Este artigo se propõe a analisar tais aspectos do atual paradigma de C2 no nível operacional e, com base neles, apresentar soluções de C2 passíveis de emprego prático no Sistema de Gerenciamento da Amazônia Azul (SisGAAz), um dos desafios fundamentais da Marinha do Brasil.

A ERA DA INFORMAÇÃO E O COMANDO E CONTROLE

A Era Industrial acabou e o mundo entrou na Era da Informação. A diferença entre o vencedor e o derrotado não se faz mais pela capacidade de produzir meios em linhas de montagem, mas sim pela superioridade de informação.

> A tecnologia da informação é o DNA da Era da Informação – o bloco de construção fundamental dos competidores dominantes (ALBERTS, GARSTKA; STEIN 2005, p. 15).

Com o advento da tecnologia da informação (TI), a massa de dados dos problemas são processadas por equipes, que trabalham sobre sistemas e redes, de modo a disponibilizar soluções ótimas ao decisor. O que conta atualmente é a Superioridade de Informação que permite o C2 ser mais eficiente e capaz de fazer aplicar o fator força no local, momento e intensidade adequados.

2 A definição de Operação de Informação é apresentada na página 5 deste artigo.

Nos navios de nossa marinha, as informações decorrentes do esclarecimento são concentradas e avaliadas nos Centros de Operações de Combate (COC). Tais informações são obtidas por intermédio do emprego de sensores, aeronaves orgânicas, linhas de comunicações, link de dados, rede de computadores e monitores. A partir da avaliação dessas informações pela equipe do COC, o Comandante do navio busca tomar a melhor decisão em ações reais e em exercícios.

Mas o desafio de C2 é considerável, há que se decidir em meio de uma quantidade significativa de informações que os sistemas disponibilizam. Algumas vezes é preciso decidir em curtíssimo espaço de tempo, como nos casos dos navios norte-americanos USS Stark[3] e USS Vincennes[4] que obtiveram a detecção de aeronave fechando ameaçadoramente no Golfo Pérsico na década de 1980. O descrédito na possibilidade de ataque, a partir dos dados disponíveis, possibilitou que o Stark fosse atingido por dois mísseis Exocet lançados por um caça Iraquiano. Já o Vincennes acabou derrubando um voo comercial inocente. Em outras palavras, as informações prestadas devem ser relevantes, corretas e passadas a tempo de permitir a reação.

> Nós podemos observar que informação tem as dimensões de relevância, acurácia e oportunidade. Por isso um limite superior no domínio da informação é atingido quando a relevância, precisão e oportunidade chegam a cem por cento (ALBERTS; GARSTKA; STEIN, 2005, p. 15).

Certamente, nos casos do Vincennes e do Stark tais parâmetros não atingiram cem por cento. São curiosos os fatos de o Stark não ter derrubado a aeronave inimiga e ter tido seu navio avariado, e de o Vincennes ter feito o contrário e também ter se dado mal, abatendo uma aeronave cheia de inocentes. Mas, ambos os Comandantes dos navios não tinham a totalidade das informações corretas. Um competidor dominante tem Superioridade de Informação quando os parâmetros de

3 USA. Cruizer-Destroyer Group Two. Formal Investigation into the Circunstances surrounding the Attack on the USS Stark (FFG31) on may 1987, 1'987, p. 2. Disponível em: <www.dod.gov/pubs/foi/operation_and_plans/USS_Liberty_Pueblo_Stark/65rev.pdf>. Acesso em: 26 Nov. 2014.

4 BUTTERFIELD, Iran Falls Short in Drive at U.N. to Condenm U.S. in Airbus case. The New York Times. 15 jul. 1988. Disponível em <www.nytimes.com/1988/07/15/world/iran-falls-short-in-drive-at-un-to-condenm-us-in-airbus-case.html>. Acesso em: 27 nov. 2014.

relevância, precisão e oportunidade das informações são superiores aos mesmos parâmetros do oponente, ou seja, quando estão mais próximos a cem por cento.

Além de resolver sua situação tática e atender ordens superiores, o Comandante do navio deve filtrar e transmitir o que é importante para o comando superior. O Comandante da Força-Tarefa, por sua vez, faz o mesmo. Desse modo, as informações chegam ao Nível Operacional, o qual tem o mesmo trabalho para que o Nível Estratégico fique a par do que lhe interessa e, então, possa assessorar o Nível Político. De fato, algumas ações do Nível Tático têm repercussões políticas. Prova disso foi o acompanhamento do Presidente dos EUA às ações do grupo de forças especiais da marinha norte-americana, os Navy Seals, que eliminaram Osama Bin Laden em 2011[5].

Nossa marinha tem o desafio de realmente inserir-se na Era da Informação. É importante que ela seja um competidor dominante e que busque a Superioridade de Informação mediante um C2 eficiente e eficaz.

Outra novidade da Era da Informação são as Operações de Informação abordadas a seguir.

OPERAÇÕES DE INFORMAÇÃO

A realidade da Era da Informação influencia o modo de planejar e conduzir as campanhas militares. De fato, as Operações de Informação são parte importante desse contexto. Num mundo globalizado, as redes e os meios de informação alcançam praticamente a todos. Até mesmo aldeias remotas e isoladas podem ser integradas à rede mundial de informação com alguns equipamentos portáteis. Forças armadas regulares, guerrilheiros, extremistas, terroristas, piratas, populações e vilarejos podem ser alvos de informações intencionalmente disseminadas que visam manipular seus comportamentos.

A importância das Operações de Informação pode ser constatada na definição do Manual Conjunto de Operações de Informação dos EUA.

5 G1. EUA anunciam a morte do terrorista Osama bin Laden no Paquistão. 02 Mai. 2011. Disponível em < http://g1.globo.com/mundo/noticia/2011/05/obama-confirma-morte-de-osama-bin-laden.html>. Acesso em 02 Dez. 2014.

> O emprego integrado, durante operações militares, de capacidades relacionadas às informações em harmonia com outras linhas de operação, para influenciar, romper, corromper, ou usurpar o processo de tomada de decisões de adversários e de potenciais adversários, enquanto protege o nosso próprio processo (USA, 2011, p. GL-3).

Além de poder ser aplicada contra uma vasta gama de públicos-alvo, as Operações de Informação podem atuar sobre o C2. Os segredos mais importantes, as verdadeiras intenções do comando podem ser protegidos pelas Operações de Informação. Tais operações ainda podem extrair informações valiosas do oponente, atribuir o ônus de agressor ao inimigo e iludi-lo de modo a consolidar uma situação vantajosa às nossas forças.

Um exemplo de dissimulação, que se constituiu em Operação de Informação bem-sucedida, foi a imobilização da Guarda Republicana de Saddam Russein[6] por meio de uma Demonstração Anfíbia realizada pelas forças de Coalizão na Primeira Guerra do Golfo. Na ocasião, a simples movimentação da Força-Tarefa Anfíbia em direção à costa foi suficiente para fixar a Guarda Republicana num local distante dos reais objetivos operacionais da Coalizão, facilitando sobremaneira a campanha como um todo.

Fica claro que as Operações de Informação são ferramentas ao planejamento e execução de campanhas. É evidente que tais operações nem sempre dependem de sofisticados recursos de TI. Movimentação de forças, notícias de jornal, panfletos, boatos, transmissões de rádio simuladas são alguns exemplos.

O anexo de Operações de Informação de nossa Doutrina de Operações Conjuntas prevê o emprego da Comunicação Social, das Operações Psicológicas, da Defesa Cibernética, da Guerra Eletrônica, do Despistamento, da Segurança da Informação e da destruição física do sistema de C2 do oponente (Doutrina de Operações Conjuntas, 2011, p. 179).

As Operações de Informação já constam da Doutrina Básica da Marinha[7]. O domínio continuado da TI, envolvida nas redes mais

6 JUNOR, Walter Félix Cardoso. Desinformação - Manipulação e Engano. Varican. Florianópolis, 2 Set. 2000. Disponível em < http://www.varican.xpg.com.br/varican/Seguranca/desin_maneng.HTM > Acesso em: 02 dez. 2014.

7 BRASIL.Estado maior da Armada. EMA-305:Doutrina Básica da Marinha (DBM) 2ª revisão. Brasília, 2014. p. A-18.

sofisticadas, é um grande desafio. Mas, talvez seja ainda mais importante saber aplicar as Operações de Informação com perspicácia e criatividade, de modo a contribuir para o atingimento do estado final desejado numa campanha, objeto do planejamento operacional.

A ideia de informação nos remete às redes, que atualmente se aplicam ao conceito de Guerra Centrada em redes, doravante abordado.

GUERRA CENTRADA EM REDES (GCR)

Com o advento da Era da Informação, a Guerra, antes vislumbrada como centrada em plataformas, tais como blindados, navios e aeronaves, passou a ter a possibilidade de ser encarada como centrada em redes de informação. Assim, como a internet permitiu ligar os computadores pessoais em uma extensa rede, a troca de dados por meio de links entre plataformas de combate amplia o alcance e a capacidade de combate de uma força.

> GCR é um conceito de superioridade de informação para operações que gera incrementado poder de combate por colocar em rede sensores, decisores e disparadores para obter compartilhada consciência situacional, aumentada velocidade de comando, maior tempo de operações, maior letalidade, incrementada sobrevivência e um grau de sincronização. Em essência, GCR traduz superioridade de informação em poder de combate por ligar efetivamente entidades reconhecíveis no espaço de batalha (ALBERTS, GARSTKA; STEIN, 2005, p. 2).

Equipamentos de troca automática de dados (os conhecidos links de dados), rádios e procedimentos padronizados de comunicações permitem o estabelecimento de uma verdadeira rede de informações entre plataformas e decisores, todos entre si. Dentre os oponentes, terá vantagem aquele que obtiver superioridade de informações a partir de sua rede. Tal superioridade de informações constitui-se da avaliação de dados mais precisos, oportunos e relevantes.

Na Batalha da Inglaterra, durante a Segunda Guerra Mundial, caças britânicos foram direcionados contra os bombardeiros alemães

pela rede de radares do sistema de defesa aérea da Royal Air Force (RAF)[8], o que salvou o Reino Unido de uma invasão inimiga. Sem dúvida alguma, o poder de combate daqueles caças foi explorado ao máximo graças à troca de informações em rede e em tempo adequado. Hoje, o link de dados é uma realidade que disponibiliza a uma plataforma as informações de sensores de outras plataformas, constituindo a distribuição da consciência situacional, que também alimenta os centros de C2 dos Comandos superiores.

Quando plataformas atuam em rede, há um efeito sinérgico que amplia o alcance e a eficácia da força como um todo. A distribuição da consciência situacional de uma grande área pode se dar por intermédio das redes de links automáticos de dados e de uma variedade de outras redes constituídas por meio de rádios, telefones, fax, internet, canais via satélite e aeronaves. A fricção e o nevoeiro da guerra podem ser reduzidos por meio do emprego da GCR, pois uma maior quantidade de informação é disponibilizada e avaliada ao conjunto de decisores. Tal fato clareia a percepção da situação e evita inconvenientes. A incerteza é diminuída, o que faz com que o ciclo de observar, orientar, decidir e agir (OODA), característico do C2, seja mais rápido. Uma vez que o ciclo de C2 é mais rápido, a força leva vantagem contra o oponente.

Meios das forças armadas pelo mundo, assim como de nossa marinha, são dotados de equipamentos que permitem o emprego da GCR. Contudo, aeronaves e mensageiros podem servir de importante opção para a transmissão de mensagens, em que pese os avanços tecnológicos que permitem o estabelecimento de conexões extremamente rápidas e seguras, a exemplo dos satélites militares e comerciais e dos rádios de HF com varredura automática de frequência. Principalmente as aeronaves, graças às suas velocidades e capacidade de servir de ponte de comunicações, podem garantir comunicações confiáveis em ambientes monitorados pelo inimigo. Isso é especialmente relevante quando não dispomos de satélites próprios e estamos sujeitos à localização por meio de Estações radiogoniométricas inimigas. Satélites de terceiros podem servir de porta de entrada para a interceptação de nossas comunicações e o trabalho de quebra de nossas cifras automáticas, com o consequente conhecimento do conteúdo de nossas mensagens. Uma aeronave preparada pode vir a constituir um meio especial de comunicações prioritário.

8 UNITED KINGDOM. Royoal Air Force. A Short History of Royal Air Force Chapter 3-The Second World War 1939-45, p.102. Disponível em: <www.raf.mod.uk/rafcms/mediafiles/E21d57c4_9913_5321_bb9830fdbb762b4e.pdf>. Acesso em: 29 nov. 2014.

O desafio é ampliar ao máximo o alcance das redes por meio de equipamentos e meios que permitam a troca de dados entre o maior número de forças que venham a atuar em conjunto.

Em seguida, analisaremos outro aspecto do paradigma de C2 atrelado à TI: a Guerra Cibernética.

GUERRA CIBERNÉTICA

Outra novidade da Era da Informação é a Guerra Cibernética, que tem o potencial de interromper o ciclo de C2 mediante ações sobre os recursos de TI da infraestrutura dos centros de C2 e respectivas redes e terminais. Os modernos centros de C2 são constituídos de computadores em rede que recebem informações de fontes locais e remotas. Tratam-se de excelentes alvos à Guerra Cibernética por definição.

> Guerra Cibernética é a não autorizada penetração por, ou em nome de, ou em apoio a um governo em computador ou rede de outra nação, ou qualquer outra atividade afetando um sistema computacional, no qual o propósito é incluir, alterar ou falsificar dado, ou causar a interrupção ou dano a um computador, ou dispositivo de rede, ou objetos que um computador controla (CLARKE; KNAKE, 2012, p. 151).

Há vários exemplos recentes de Guerra Cibernética, como os ataques à Estônia[9] em 2007 e à Geórgia[10] em 2008, assim como aquele direcionado às instalações nucleares do Irã, provavelmente com o "worm Stuxnet"[11] em 2010.

Pode-se imaginar o impacto sobre uma campanha no caso de um ataque cibernético que consiga interromper o fluxo de informações entre os níveis tático, operacional e estratégico. Ainda pior seria se tais informações fossem alteradas de modo a gerar situações favoráveis ao inimigo sem que ninguém percebesse.

---

9 TRAYNOR, Ian. Russia accused of unleashing cyberwar to disable Estonia.The Guardian. Londres, 17 Mai. 2007. Disponível em: <www.theguardian.com/world/2007/may/17/topstories3.russia. Acesso em: 27 nov 2014.

10 HOLLIS, David. Cyber War Case Study: Georgia 2008. Disponível em: <http://smalwarsjournal.com/blog/docs-temp/639-hollis.pdf>. Acesso em: 25 nov. 2014.

11 MACMILLAN, Robert. Was Stuxnet built to attack Iran's nuclear program? Infoworld.21 Set. 2010. Disponível em: <www.infoworld.com/article/2626198/hacking/ was-stuxnet-built-to-attack-iran-s-nuclear-program.html>. Acesso em: 24 nov. 2014.

A ameaça pode ir além do comprometimento do fluxo de C2. Recentes sistemas controlados por computador podem ser avariados pela ação de vírus injetados maliciosamente. Tais vírus modificam os programas controladores, denominados códigos-fonte, das máquinas que estão sendo atacadas, de modo que obedeçam instruções intrusas que provoquem determinado efeito pernicioso programado pelo inimigo. Armamentos, propulsores, centrais de energia são alguns exemplos de sistemas de meios táticos que podem ser danificados caso o código fonte dos respectivos sistemas de controle venham a ser corrompidos, a exemplo do que o Stuxnet fez com a central nuclear iraniana. E, obviamente, tal ameaça estende-se às infraestruturas de um Estado que sejam gerenciadas por computador.

Mas o que fazer para evitar um ataque cibernético? Sem dúvida alguma é um grande desafio, e nossa marinha insere-se nesse contexto. Adestramento sobre comportamentos seguros dos operadores e o uso de sistemas exclusivos e inéditos são os primeiros passos desde o tempo de paz. A atualização dos softwares e o reajuste da configuração dos sistemas são igualmente importantes.

Os sistemas mais seguros são aqueles que os "hackers" ainda não tiveram tempo de desvendar o código-fonte e alterá-lo de acordo com suas intenções adversas. Daí, o valor de dispor de uma equipe capaz de desenvolver sistemas inéditos e exclusivos, manter atualizados os softwares e reajustar configurações de rubs, switches e demais vulnerabilidades.
Ou seja, na atualidade, a expertise em segurança da informação e o desenvolvimento de softwares próprios são de fundamental importância para a defesa das redes e centros de C2 e outros potenciais alvos cibernéticos.

Outro assunto atualíssimo na esfera do C2 são os indicadores empregados para medir o desempenho das forças numa campanha.

INDICADORES

Hoje em dia, as campanhas militares têm grande visibilidade na mídia nacional e internacional. Esse fato gera pressões políticas e econômicas no sentido de que o esforço bélico seja otimizado. Espera-se que o número de baixas civis e militares seja mínimo, que não haja desperdício de recursos financeiros e materiais e que o estado final desejado seja rapidamente atingido.

O Comando do Teatro de Operações, por intermédio de seu Estado-Maior, define indicadores, durante o planejamento de uma

campanha, que servirão para o controle das fases e das operações planejadas. O próprio apoio da mídia em prol de nossa missão pode ser trabalhado em termos de indicadores.

> O contínuo controle e avaliação das ações planejadas se fazem por meio de ferramentas denominadas indicadores, os quais constituem dados quantitativos ou qualitativos que permitem ao Estado-Maior Conjunto acompanhar o desenvolvimento das operações, comparando os resultados obtidos com o planejamento da campanha (BRASIL, 2011, p. 87).

Busca-se, por meio de indicadores, verificar se os efeitos desejados estão sendo atingidos e se as tarefas estão sendo executadas de maneira correta. Desse modo, procura-se manter o desenvolvimento da campanha dentro de parâmetros aceitáveis em termos militares. Hoje, tal aceitabilidade leva em consideração a repercussão política, econômica e social, uma vez que os meios de comunicação levam a todos parcela considerável das ocorrências nas operações. O simples fato de negar informações do ocorrido é motivo de matéria e discussões na mídia, que podem não ser do interesse do Comandante do Teatro de Operações.

Os indicadores referem-se a metas a serem atingidas, traduzidas em percentuais quantificáveis ou fatos qualitativos. Como indicador podemos exemplificar o seguinte: 95% dos navios mercantes que suspenderam do porto A devem chegar ao porto B. Outro exemplo: a cidade B deve estar abastecida de combustível para dois meses por meio de dois petroleiros.

Podem ser criados indicadores para acompanhamento do atingimento de pontos decisivos e de condições para mudança de fase da campanha. Esses últimos definem se a atitude geral das forças envolvidas pode ser mudada. Ou seja, são de importância capital para o controle da campanha. A verificação da destruição ou neutralização de alvos é fonte fundamental para a gerência dos indicadores. Hoje, os veículos aéreos não tripulados (VANT), ou aeronaves remotamente pilotadas (ARP), são ferramentas para missões de alto risco e levantamento da consciência situacional em profundidade, muitas vezes necessária ao levantamento dos parâmetros dos indicadores.

Mas os indicadores não devem ser encarados como os propósitos finais e imutáveis de cada fase. Não se trata de elementos de comando e sim de controle. É importante que os indicadores não se tornem metas a

serem atingidas cegamente, a exemplo do que ocorreu na Guerra do Vietnã, quando os corpos de combatentes inimigos mortos eram contados como indicador de desempenho[12]. O resultado de se buscar grosseiramente tal indicador foi uma carnificina que atrapalhava a obtenção do estado final desejado naquele conflito.

Hoje, existe uma doutrina conjunta nacional que versa sobre indicadores. Mas, permanece o desafio à Marinha do Brasil em desenvolvê-la e incorporá-la, pois trata-se de importante ferramenta de planejamento e controle.

A AGILIDADE DE C2

O comandar e o controlar se fazem por meio de comunicações, e seus cinco tradicionais requisitos, quais sejam confiabilidade, segurança, rapidez, flexibilidade e integração, contam agora com um sexto integrante: a agilidade de C2. Trata-se de um novo conceito em que toda a estrutura de C2 deve ser pensada e modificada de acordo com a alteração significativa da situação ou mesmo da missão. Vai muito além da simples necessidade de se dispor de canais alternativos para a transmissão de mensagens.

> A Teoria da Agilidade sustenta que abordagens de C2 diferem em três fundamentais formas:
> 1) como os direitos de decisão são alocados;
> 2) como as entidades interagem umas com as outras;
> 3) como a informação é distribuída (USA, 2014, p. 4).

A doutrina deve ser suficientemente flexível para que a estrutura de C2 sofra modificações de acordo com os desafios da situação. O quanto cada nível decisório será mais autônomo? Quais relações de comando serão estabelecidas? Como a rede de informações entre os decisores será irrigada? Todas essas são questões que devem ser solucionadas não somente pelo Estado-Maior do Comandante do Teatro de Operações, mas sim por cada direção de nível de condução da guerra.

Por exemplo, que autonomia será dada ao comandante de um submarino nuclear de ataque? Como irrigar esse submarino com informações e ordens? Muito provavelmente, decisões de impacto político estratégico deverão ser repassadas diretamente do nível político

12 DADDIS, Gregory A., 2009, p.iii.

para o tático. Isso aconteceu na Guerra das Malvinas em 1982, ocasião em que o Submarino britânico Conqueror Britânico afundou o Cruzador argentino General Belgrano em alto-mar após receber aprovação para tal da então Primeira-Ministra Margaret Thatcher[13]. A ação foi realizada fora da Zona de Exclusão estabelecida pelo Reino Unido e longe de qualquer ponto focal. Esse afundamento teve efeito dissuasório imediato, pois os navios argentinos deixaram a área de operações, voltando para sua base. Assim, comprovou-se a importância do submarino nuclear de ataque e do C2 ágil para a guerra no mar. Isso vale para a aplicação da força dentro e fora da Amazônia Azul, assim como para dissuasão de eventuais oponentes.

Será que a simples existência das três Forças Componentes Aérea, Naval e Terrestre resolverá sempre todos os tipos de conflitos que o Comandante do Teatro de Operações terá que encarar? Certamente não, segundo a Teoria da Agilidade de C2 apresentada pelo Programa de Pesquisa de C2 do Departamento de Defesa dos Estados Unidos da América[14].

Opções como a Força Naval Componente Submarina e a Força Conjunta de Operações Especiais podem e devem ser pensadas para cenários específicos. Mas com os devidos cuidados. Não se deve ferir a unidade de esforços e o cumprimento da estratégia geral concebida. De nada adiantam mais Comandos Conjuntos se for perdido o foco para o cumprimento da missão.

Uma Operação de Garantia da Lei e da Ordem (GLO), como ocorre hoje na comunidade da Maré na cidade do Rio de Janeiro, demanda toda uma estrutura de C2 específica e adaptada. As operações naquele ambiente, e com os atores específicos, exigem a capacidade de unir esforços para o cumprimento da missão e o atingimento do estado final desejado, qual seja, a pacificação da comunidade.

No contexto da Agilidade de C2, é bem-vinda a atuação inter-agências, abrangendo a Força Nacional, a Receita Federal as Polícias Federal e Estaduais, o IBAMA, a Defesa Civil, a Imprensa e até mesmo empresas como a Petrobras. A Amazônia Azul é passível de questões que envolvam a defesa da Pátria, o tráfico ilícito, as catástrofes ambientais e até mesmo a pirataria.

13 THE PORTSMOUTH NEWS. Belgrano posed a real threat to fleet. Portsmouth, 2 Abr. 2007. Disponível em: <www.portsmouth.co.uk/nostalgia/belgrano-posed-a-real-threat--to-fleet-1-1271951>. Acesso em: 28 nov. 2014.

14 USA, 2014, p. 4.

Qualquer que seja a campanha ou operação, há que se chamar atenção para que não sejam cometidos erros triviais como a concentração dos Centros de C2 em uma mesma localidade e a inexistência de Centros de C2 alternativos. Os Centros de C2 são alvos naturais para as forças inimigas que devem ser bem protegidos e planejados.

A atribuição de tarefas aos comandos subordinados deve seguir as doutrinas básicas das três forças. Mas, é fundamental para a devida condução da campanha que tais tarefas sejam expressas em termos de efeito desejado. Assim, definimos aos subordinados o que queremos sem tirar a liberdade de planejar e atuar de acordo com seu entendimento e possibilidades.

A coordenação das forças componentes deve ser feita por janelas de tempo ou por áreas de atuação de modo a evitar a interferência mútua e o fratricídio. Ainda no campo do controle, deve-se atentar para as rotas de navegação e as aerovias. É importante desviar rotas de forma a evitar mortes de inocentes. Relembra-se a derrubada da aeronave da Malasian Airlines na Ucrânia este ano[15].

A expedição da Lista Integrada e Priorizada de Alvos (LIPA) a serem batidos pelas Forças Componentes deve procurar balancear a quantidade de alvos distribuída para cada Força. É de grande valia atribuir alvos em profundidade do espaço inimigo não somente à Força Aérea Componente, mas também às Operações Especiais e aos submarinos, as quais poderão assumir parte considerável do esforço. Isso vale principalmente para o caso em que a Força Aérea Componente não tiver uma comparação de poderes combatentes muito favorável.

Outro recurso fundamental é a emissão da Ordem Preparatória ao final da análise da missão. Tal diretiva permite ao Comando subordinado antecipar providências e fornecer subsídios ao Comando Operacional quanto às informações necessárias ao estabelecimento da exequibilidade de linhas de ação.

A estrutura de C2 estabelecida pode admitir sua própria mutação durante a evolução do conflito. Fases diferentes de uma campanha correspondem a cenários diferentes e, nem sempre, a mesma estrutura de C2 será a mais eficiente para cada situação. A capacidade de modificar os direitos de decisão, as relações de comando e a distribuição de informações

15 G1. Avião da Malaysia Airlines com 298 pessoas a bordo cai na Ucrânia. São Paulo, 17 Jul. 2014. Disponível em: <g1.globo.com/mundo/noticia/2014/07/aviao-da-malasia-com-295-bordo-cai-na-ucrania-diz-agencia.html>. Acesso em: 28 nov. 2014.

constitui-se na própria Agilidade de C2, fundamental para o C2 do emprego da força na atualidade.

Uma vez analisados os principais aspectos do atual paradigma de C2, partimos agora para a apresentação de soluções de C2 para o SisGAAz com base no escrito até aqui.

SOLUÇÕES DE C2 PARA O SisGAAz

A Marinha do Brasil vislumbrou o SisGAAz em consonância com a diretriz número dois da Estratégia Nacional de Defesa.

> 2. Organizar as Forças Armadas sob a égide do trinômio monitoramento/controle, mobilidade e presença. Esse triplo imperativo vale, com as adaptações cabíveis, para cada Força. Do trinômio resulta a definição das capacitações operacionais de cada uma das Forças (BRASIL, 2008, p. 11).

O SisGAAz cobrirá toda a Amazônia Azul[16] e inclusive áreas oceânicas, litorâneas e fluviais[17]. Em virtude do enorme espaço a ser monitorado, haverá a necessidade de grande esforço de comandar e controlar os meios e sistemas envolvidos.

Os conceitos de C2 apresentados neste trabalho são passíveis de aplicação nos esforços de organização e adaptação das Forças Armadas para a tarefa de vigiar a Amazônia Azul e as áreas oceânicas, litorâneas e fluviais a serem cobertas pelo sistema. O desenvolvimento e o emprego do SisGAAz podem e devem absorver os Sistemas de C2 no estado da arte da Era da Informação, as Operações de Informação, os conceitos e as aplicações da Guerra Centrada em Redes, os Recursos de Guerra Cibernética, o emprego de Indicadores e da Agilidade de C2. Embora não esgote o assunto, pode-se destacar a aplicabilidade das seguintes soluções de C2, a partir dos aspectos do atual paradigma de C2 (em itálico):

— Busca pela Superioridade de Informação: *Guerra centrada em Redes;*

— Adaptação da Estrutura de C2 de acordo com a situação: *Agilidade de C2*;

— Redes de informação: *Guerra Centrada em Redes*;

— Vigilância e comunicações por satélite autóctones: *Guerra Centrada em Redes*;

16 Disponível em: <https://www.marinha.mil.br/sites/default/files/hotsites/amz_azul/html/definicao.html>. Acesso em: 4 dez. 2014.

17 JUNIOR, Francisco Antonio de Oliveira, 2013, p. 45.

— Rede de comunicações em HF: *Guerra Centrada em Redes*;

— Rede de estações radiogoniométricas de alta frequência: *Guerra Centrada em Redes*;

— Link de dados entre meios e centros de comando e controle: *Era da Informação;*

— Modernos centros de C2: *Era da Informação*;

— Sistemas computacionais com elevada capacidade: *Era da Informação*;

— Navios dotados de COC: *Era da Informação*;

— Aeronaves: *Guerra Centrada em Redes*;

—VANTs: *Indicadores*;

— Submarinos nucleares de ataque: *Agilidade de C2*;

— Equipes de defesa e de ataque cibernético: *Guerra Cibernética;*

— Equipes de operações especiais prontas: *Agilidade de C2*;

— Equipe de operações de informações: *Operações de Informação*;

— Indicadores confiáveis para a consciência situacional: *Indicadores;*

— Coordenação de forças componentes por áreas e janelas de tempo: *Agilidade de C2*;

— Controle das rotas marítimas e aéreas: *Agilidade de C2*;

— Atuação inter-agências: *Agilidade de C2*.

Com as aplicações dessas soluções certamente teríamos um SisGAAz mais eficiente.

A relevância dessas soluções aqui apresentadas decorre do fato de que o SisGAAz se constitui em uma questão de C2 fundamental para a Marinha do Brasil e para o país como um todo.

CONCLUSÃO

A Era da Informação provocou a evolução do paradigma de C2, o que trouxe uma série de desafios à nossa Marinha para que ela se mantenha em condições de realizar suas tarefas.

A Marinha do Brasil deve buscar continuamente manter-se na crista da onda da Era da Informação, não se deixando superar por competidores. A solução não repousa em apenas comprar novos computadores e recursos de TI. A chave é ter a Superioridade de Informação mediante o C2 eficiente e eficaz.

A doutrina das Operações de Informação está em desenvolvimento e seu domínio passa pela aplicação da perspicácia e da criatividade sobre

a massa de dados disponível, de modo a moldar, a nosso favor, as atitudes de amigos e possíveis inimigos.

Existe o desafio de ampliar ao máximo o alcance dos conceitos da GCR por meio de equipamentos que permitam a efetiva interoperabilidade entre os centros de C2, os meios da força naval e das forças amigas.

Na atualidade, a expertise em segurança da informação e o desenvolvimento de softwares próprios são de fundamental importância para a defesa das redes e centros de C2. O adestramento sobre comportamentos seguros dos operadores e o uso de sistemas exclusivos e inéditos são bons caminhos para evitar ataques cibernéticos. Devem ser evitados o descuido de operadores e o emprego de sistemas, os quais os oponentes já tiveram tempo de descobrir como corromper.

O emprego de indicadores é uma importante ferramenta de planejamento e controle a ser empregada cuidadosamente nas grandes operações e campanhas que nossa marinha venha a participar.

A agilidade de C2 surge como novo requisito para a condução da aplicação da força. A doutrina deve atender questões como alocar direitos de direção, estabelecer relações e distribuir informação.

A aplicação de soluções da Era da Informação, de Operações de Informação, de Guerra Centrada em Redes, de Guerra Cibernética, de Indicadores e de Agilidade de C2 no desenvolvimento do SisGAAz certamente o tornaria mais efetivo e o colocaria em sintonia com o atual paradigma de C2.

REFERÊNCIAS

ALBERTS, David S.; GARSTKA, John J.; STEIN, Frederick P. *Network Centric Warfare: developing and leveraging information superiority*. Washington: CCRP Publication Series, 2005.

BUTTERFIELD, *Iran Falls Short in Drive at U.N. to Condenm U.S. in Airbus case*. The New York Times. 15 jul. 1988. Disponível em: <www.nytimes.com/1988/07/15/world/iran-falls-short-in-drive-at-un-to-condenm-us-in-airbus-case.html>. Acesso em: 27 nov. 2014.

BRASIL. Ministério da Defesa. *Estratégia Nacional de Defesa*. Brasília, 2012.

_____. *MD30-M-01, Doutrina de Operações Conjuntas*, *1º Volume*. Brasília, 2011.

_____. *MD31-M-03*, *Doutrina para o Sistema Militar de Comando e Controle*. Brasília, 2014.

BRASIL. Estado-Maior da Armada. *EMA-305: Doutrina Básica da Marinha, rev. 2.* Brasília, 2014.

_____. EMA-331: *Manual de Planejamento Operativo da Marinha, Volume III, O Trabalho das Seções de Estado-Maior*. Brasília, 2006.

CLARKE, Richard A.; KNAKE, Robert K. *Cyber War:* the next threat to national security and what to do about it. New York: Harper Collins Publishers, 2012.

COAKLEY, Thomas P. *Command and Control for War and Peace*. Washington: National Defence University Press, 1992.

DADDIS, Gregory A. *No sure victory:* measuring U.S. Army Effectiveness and Progress in the Vietnam War. 2009. 412 f. Dissertação – University of North Carolina at Chapel Hill, 2009.

MACMILLAN, Robert. Was Stuxnet built to attack Iran's nuclear program? *Infoworld.* 21 Set. 2010. Disponível em: < www.infoworld.com/article/2626198/hacking/ was-stuxnet-built-to-attack-iran-s-nuclear-program.html>. Acesso em: 24 nov. 2014.

G1. *Avião da Malaysia Airlines com 298 pessoas a bordo cai na Ucrânia*. São Paulo, 17 Jul. 2014. Disponível em: < g1.globo.com/mundo/noticia/2014/07/aviao-da-malasia-com-295-bordo-cai-na-ucrania-diz-agencia.html>. Acesso em: 28 Nov. 2014.

G1. *EUA anunciam a morte do terrorista osama bin Laden no Paquistão*. 02 mai. 2011. Disponível em: < http://g1.globo.com/mundo/noticia/2011/05/obama-confirma-morte-de-osama-bin-laden.html>. Acesso em: 2 dez. 2014.

HOLLIS, David. Cyber War Case Study: Georgia 2008. *Small Wars Journal*, 6 Jan., 2011. Disponível em: < http://smalwarsjournal.com/blog/docs-temp/639-hollis.pdf>. Acesso em: 25 nov. 2014.

JUNIOR, Francisco Antonio de Oliveira. *As Perspectivas da Concepção Atual do Sistema de Gerenciamento da Amazônia Azul (SisGAAz) para o Monitoramento e Controle das Águas Jurisdicionais Brasileiras (AJB)*. 2013. 93 f. Dissertação (Mestrado em Ciências Navais) – Escola de Guerra Naval. Rio de Janeiro, 2013.

JUNIOR, Walter Félix Cardoso. *Desinformação - Manipulação e Engano*. Varican. Florianópolis, 2 Set. 2000. Disponível em: < http://www.varican.xpg.com.br/varican/Seguranca/Desin_ maneng.htm > Acesso em: 2 dez. 2014.

UNITED KINGDOM. Royoal Air Force. *A Short History of Royal Air Force Chapter 3-The Second World War 1939-45*. Disponível em: < www.raf.mod.uk/rafcms/mediafiles/E21d57c499135321bb9830fdbb762b4e.pdf. Acesso em: 29 nov. 2014.

USA. Department of Defense. Cruiser-Destroyer Group Two. *Formal Investigation into the circunstances surrouding the attack on the USS Stark (FFG31) on 17 May 1987*. Disponível em: < www.dod.gov/pubs/foi/operationandplans/USS_Liberty_Pueblo_Stark/65rev.pdf. Acesso em: 26 nov. 2014.

USA. Department of Defense. *Joint Publication 3-0, Joint Operations*. Washington, 2011.

USA. Department of Defense. *Joint Publication 5-0, Joint Operation Planning*. Washington, 2011.

USA. Department of Defense Command and Control Research Program. *C2 by design: A Handbook for Putting Command and Control Agility Theory Into Practice*. Washington, 2014.

USA. Department of the Navy. *NWP 5-01, Navy Planning*. Norfolk, 2013.

THE PORTSMOUTH NEWS. *Belgrano posed a real threat to fleet. Portsmouth,* 2 Abr. 2007. Disponível em: < www.portsmouth.co.uk/nostalgia/belgrano-posed-a-real-threat-to-fleet-1-1271951>. Acesso em: 28 nov. 2014.

TRAYNOR, Ian. *Russia accused of unleashing cyberwar to disable Estonia*.The Guardian. Londres, 17 Mai. 2007. Disponível em: < www.theguardian.com/world/2007/may/17/topstories.russia. Acesso em: 27 nov. 2014.

Recebido em: 17/10/2014
Aceito em: 10/04/2015