ESCOLA DE GUERRA NAVAL

CC JÉMISSON BEAUTRIX

Os desafios da integração do Ciberespaço e do Campo Informacional na Arte Operacional Militar Moderna.

Rio de Janeiro

2024

CC JÉMISSON BEAUTRIX

Os desafios da integração do Ciberespaço e do Campo Informacional na Arte Operacional Militar Moderna.

Dissertação apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientador: CMG (RM1) Luis Fernando Nogueira Pompeu

Rio de Janeiro

Escola de Guerra Naval

2024

AGRADECIMENTOS

Através dos tempos, os oceanos forjaram inúmeras gerações de marinheiros. Ilustres ou anônimos, foram testemunhas de seu tempo, construtores de nações, artesãos da História. Com os olhos fixos no horizonte, eles ampliaram os limites do mundo conhecido graças à sua coragem, ao gosto pelas novas técnicas e à sede de aventuras. Hoje, sinto o orgulho ao seguir seus passos.

Ao meu orientador, Capitão de Mar e Guerra (RM1) Luis Fernando Nogueira Pompeu, pela paciência, pelos conselhos preciosos ao longo desse trabalho de pesquisa.

Ao meu pai, que me deu tudo quando a vida mostrou seu lado o mais duro.

À minha mãe, por tudo o que ela me ofereceu desde o primeiro dia em que me tomou pela mão.

Às minhas filhas, Lili-Jeanne e Anabelle, que me dão cada dia a maior alegria de ser pai.

À Julita, la femme de ma vie.

RESUMO

Esta dissertação aborda a nova percepção da arte operacional nos campos de confrontação emergentes desde o estágio da competição entre nações. O foco principal é a integração das características do ciberespaço e do campo informacional nos processos de planejamento militar no nível operacional.

O trabalho começa com uma análise do cenário mundial pós-Guerra Fria, destacando a instabilidade global crescente devido a fatores como mudanças climáticas, explosão demográfica, fanatismo religioso e novas ameaças tecnológicas. A introdução contextualiza a necessidade de adaptação das forças armadas a novas dimensões de combate, particularmente o ciberespaço e o campo informacional.

A dissertação explora a origem e os conceitos-chave da arte operacional, diferenciando-a de estratégias militares tradicionais como as de Napoleão e Clausewitz. A arte operacional é apresentada como uma disciplina complexa que se desenvolveu entre as duas guerras mundiais, especialmente na Rússia, e que se tornou essencial no planejamento militar moderno.

A pesquisa detalha os desafios específicos do ciberespaço e do campo informacional. Estas novas dimensões de combate são analisadas em termos de suas características únicas, princípios e desafios. Exemplos de situações operacionais recentes são usados para ilustrar a aplicação prática desses conceitos.

Enfim, a análise conecta a parte teórica da arte operacional com os desafios do ciberespaço e do campo informacional. As conexões ressaltam novas realidades que se impõem à iniciativa, à incerteza, à permanência e ao comando. Essas noções são conectadas aos elementos discutidos nos capítulos teóricos e práticos.

A dissertação conclui com reflexões sobre como aprimorar a compreensão e aplicação da arte operacional em um contexto multidomínio. São sugeridos eixos de reflexão para melhorar a eficácia do planejamento militar frente às novas ameaças e oportunidades tecnológicas.

Palavras-chave: Arte operacional, ciberespaço, campo informacional, planejamento militar, nível operacional.

DECLARAÇÃO DA NÃO EXISTÊNCIA DE APROPRIAÇÃO INTELECTUAL IRREGULAR

Declaro que este trabalho acadêmico: a) corresponde ao resultado de investigação por mim desenvolvida, enquanto discente da Escola de Guerra Naval (EGN); b) é um trabalho original, ou seja, que não foi por mim anteriormente utilizado para fins acadêmicos ou quaisquer outros; c) é inédito, isto é, não foi ainda objeto de publicação; e d) é de minha integral e exclusiva autoria.

Declaro também que tenho ciência de que a utilização de ideias ou palavras de autoria de outrem, sem a devida identificação da fonte, e o uso de recursos de inteligência artificial no processo de escrita constituem grave falta ética, moral, legal e disciplinar. Ademais, assumo o compromisso de que este trabalho possa, a qualquer tempo, ser analisado para verificação de sua originalidade e ineditismo, por meio de ferramentas de detecção de similaridades ou por profissionais qualificados.

Documento assinado digitalmente
gov.br
JEMISSON ABEL BEAUTRIX
Data: 11/11/2024 22:42:25-0300
Verifique em https://validar.iti.gov.br

SUMÁRIO

1 INTRODUÇÃO 1
2 A ARTE OPERACIONAL: O ALINHAMENTO-CHAVE.....3
2.1 CHAVES DA ARTE OPERACIONAL E NOVA CONFLITUALIDADE 4
2.1.1 A arte operacional: origem e conceitos-chave. 4
2.1.2 Distinção entre *xadrez* e o *go*. 5
2.1.3 Mudança de paradigma de conflitualidade. 8
2.2 QUADRO OPERACIONAL: UM ALINHAMENTO GLOBAL.....10
2.2.1 Importância da ambição político-estratégica 10
2.2.2 O planejamento: etapa-chave entre antecipação e a ação.....12
2.2.3 O desafio da inteligência. 13
3 O CIBERESPACO: A ESTRUTURA EM CAMADA DESAFIADORA 15
3.1 O ciberespaço técnico 16
3.1.1 Características do meio 16
3.1.2 Princípio da postura permanente de cibersegurança 17
3.1.3 Desafios do planejamento de operações no ciberespaço 18
3.1.4 O episódio do início da guerra na Ucrania.....20
3.2 O campo informacional 21
3.2.1 Características do campo informacional.....21
3.2.2 O desafio dos Estados democrático : ataques informacionais. 23
3.2.3 Planejamento operacional no campo informacional 24
3.2.4 O episódio de Gossi (Mali) contra a França 26
4 CONEXÕES: AS CHAVES DO PRÓXIMO SALTO CONCEITUAL 28
4.1 As perspectivas do princípio da iniciativa 28
4.2 As perspectivas do princípio da incerteza.....30
4.3 As perspectivas do princípio da permanência 33
4.4 As perspectivas do princípio do comando 35
5 CONCLUSÃO 37

1 INTRODUÇÃO

No início de 1992, apoiando-se sobre os trabalhos de Friedrich Hegel, Alexandre Kojève e Karl Marx, Francis Fukuyama publicou o livro *"O Fim da História e o Último Homem"*[1]. Profeta do ponto final da evolução político-econômica ou golpe de publicidade ingênuo, ele interpretou a queda do muro de Berlim em 1989 e o colapso da União Soviética em 1991 como uma ruptura durável e a vitória definitiva do modelo estadunidense.

No entanto, dez anos depois, no dia 11 de setembro 2001, o mundo descobriu um colosso ocidental com pés de barro. A *pax americana* sofreu seu primeiro soco, enquanto o novo século revelava novas ameaças contra a estabilidade global. Hoje, depois de trinta anos buscando os dividendos da paz, num contexto da desinibição de várias potências regionais e a multiplicação dos focos de crise, o mundo se rearma.

A tomada de consciência é terrível: mudanças climáticas, explosão demográfica de países emergentes, contestação da ordem e do direito internacional, fanatismo religioso, retorno às estratégias beligerantes.

Ao mesmo tempo, a ruptura tecnológica digital modificou profundamente o relacionamento dentro das estruturas humanas. Paradoxalmente, se essa ruptura é uma fonte prodigiosa de oportunidades e de desenvolvimento quase sem precedentes na história, ela é também o poço sem fundo de todos os vícios, de manipulações estatais e de riscos para o acesso pelo cidadão à informação legítima. Ainda mais preocupante, não são apenas as grandes potências que são alvo das novas lógicas de influência. A soberania de todos os países democráticos está sendo visada, numa estratégia de influência que leva a um mundo multipolar instável onde o exercício da força é facilitado pela névoa da guerra e o direito é desrespeitado a partir de novas zonas cinzentas.

Desde então, para as estruturas militares, uma mutação sem precedentes está ocorrendo nos métodos de comando, na inteligência, nas doutrinas e nas armas. Em particular, as forças armadas no século XXI têm que se adaptar e investir em novas dimensões físicas que são o ciberespaço e sua camada cognitiva, o campo informacional.

---

[1] The End of History and the Last Man. Free Press, 1992. (ISBN 0-02-910975-2).

Em paralelo, essa ruptura nas mentalidades e nos métodos deve ser acompanhada de um novo paradigma, capaz de criar as condições de reflexão em cada nível de comando para oferecer capacidades adaptadas em todo o espectro de missões. Ainda glorificando os princípios de Clausewitz, Castex e Coutau-Bégarie nas escolas de guerra e nos altos estudos de estado-maior, o pensamento estratégico, operacional e tático ocidental está diante do desafio de seu tempo.

Na fronteira entre os níveis de comando estratégico e tático, o nível operacional surge como o mecanismo do uso da força favoravelmente à guerra, ou seja, uma dobradiça entre a estratégia ligada ao político e a camada combatente. Inspirado das manobras de Napoleão e dos ensinos de Clausewitz, esse nível de comando nasceu na Rússia entra as duas guerras mundiais e se tornou uma disciplina complexa. Fruto do saber-fazer de cada país, ela adotou o nome de “arte operacional” e representa o ponto focal da consciência situacional, das decisões e dos métodos, ou seja, o centro nervoso da guerra.

A pesquisa está estruturada em cinco capítulos. Ela apresenta o desafio da integração das características do ciberespaço e do campo informacional nos processos de planejamento militar do nível operacional.

Após a introdução, o desenvolvimento de uma parte teórica permitirá desenhar o que caracteriza a arte operacional e elaborar uma concepção dos alicerces deste novo contexto estratégico. Enfim, a arte operacional surgirá como um cruzamento entre vários processos: a definição de uma ambição política, a antecipação e a inteligência.

Na terceira parte, serão expostos os desafios do ciberespaço e de suas camadas técnica e cognitiva, chamado também de campo informacional. Cada camada será detalhada com suas próprias características, princípios e desafios. Esses desafios do ciberespaço técnico e do campo informacional serão ilustrados com situações operacionais recentes e sobre as quais existem informações de fontes abertas.

Na quarta parte, nós examinaremos quatro noções que representam as chaves para entendimento do desafios impostos à arte operacional pelo ciberespaço técnico e o campo informacional. A percepção de cada um das quatro noções será enriquecida por múltiplas conexões ligando elementos dos capítulos dois e três.

Enfim, o quinto capítulo apresenta as conclusões ressaltando eixos de reflexões para melhorar a compreensão da arte operacional no contexto multidomínio.

2 A ARTE OPERACIONAL: O ALINHAMENTO-CHAVE

A primeira batalha do período Neolítico e a guerra contemporânea têm um ponto comum: apesar de inovar com novas armas, o ser humano sempre quis contornar seu oponente para obter uma vantagem decisiva no combate. Assim, a partir do uso do cavalo para ampliar sua capacidade terrestre, o estrategista integrou progressivamente no seu plano o emprego de navios e de aviões para dominar seu adversário investindo em novas dimensões (Dabila, 2013).

No século XXI, caracterizado pela explosão tecnológica do digital, a mudança da era da informação à era do conhecimento fez aparecer novas dimensões não apenas físicas, mas também imateriais (Marangé, 2021).

Na nossa análise, levamos em considerações cinco meios de confrontação: a terra, o mar, o ar, o espaço extra-atmosférico e o ciberespaço. Em outras palavras, o domínio da luta se amplia do fundo do mar ao espaço extra-atmosférico, passando para um substrato cibernético sem o qual a ação é quase impossível nos outros meios. A elas se agregam duas dimensões imateriais também qualificados como campos de confrontação: o campo informacional e o campo eletromagnético (Burkhard, 2021).

Contrariamente aos campos, os meios são estruturados por um comando e controle (C2) bem definido. Além da organização das armadas, o caráter imaterial, a capacidade de longo alcance e a abordagem global que ele impõe, fazem com que um campo de confrontação não constitui uma componente. Ele é integrado nas forças sem estrutura de comando tática dedicada. A atuação em um campo transcende a visão compartimentada dos meios e cria interações mais complexas.

Essa parte representa a base teórica da pesquisa. A noção de arte operacional será introduzida apoiando-se de produções literárias, de uma visão inovadora do contexto estratégico e por meio de uma representação lúdica. Depois,

analisaremos a importância da construção de uma ambição política frente ao contexto volátil e complexo de hoje.

2.1 CHAVES DA ARTE OPERACIONAL E NOVA CONFLITUALIDADE

2.1.1 A arte operacional: origem e conceitos-chave.

Durante suas campanhas militares no início do século XIX, Napoleão se via tanto como Imperador decisor, o estrategista organizador das batalhas e o general pensador da manobra.

Um pouco mais tarde, no primeiro capítulo do seu segundo livro “Da Guerra”, Clausewitz dividia a estratégia e a tática. Por um lado, a estratégia vem do grego *stratos*, que significa armada, e *ageîn*, que significa dirigir. Por outro lado, a tática, palavra usada desde a antiguidade derivada do greco *taktikhê*, designa a organização das tropas no terreno da batalha (Bihan, 2023). Assim, elas se preocupam, respectivamente, em ganhar a guerra e em ganhar os combates.

No século XX, essa constatação inicial não resistiu à ruptura nesta pilha de responsabilidades, bem como apareceu uma maior complexidade para lidar com uma guerra na era industrial. A partir deste momento, a reflexão estratégica sentiu a falta de uma dobradiça operativa, correia de transmissão entre os objetivos da guerra e os engajamentos no terreno.

Em 1927, Alexander Svechin publicou seu livro-monumento *Estratégia*. Num contexto histórico pesado vivenciado pela Rússia[2], o General instrutor da Academia militar *Frunze* escreveu a sua própria visão da teoria da guerra. Ele foi influenciado pela politização do combate durante a recente guerra civil russa e por pensadores poderosos como Clausewitz e Karl Marx (Olsen, 2010). Tentando regrar a dialética entre o imutável/inalterável e a contingência da guerra, ele materializou uma ferramenta de gestão da violência ao benefício da guerra: a arte[3] operacional.

Essa teoria possui conceitos-chave, em termos de fundo e de forma, tomando por base os resultados dos combates como matéria-prima (Bihan, 2023). No fundo, Svechin compõe a guerra a partir de três dimensões: os objetivos definidos pelo estrategista, razões de ser da operação e rumo do caminho estratégico; um conjunto

[2] O trauma da derrota contra o Japão em 1905; primeira guerra mundial; e guerra civil de 1917 até 1921.
[3] Nesse sentido, a palavra “arte” é usada como “disciplina”.

de múltiplas ações organizadas no espaço e no tempo; e um esforço sustentado, mantendo a sequência e o ritmo de ações no tempo-duração da operação.

> "Nós podemos definir a operação como a materialização – sob a forma de uma combinação de atividades militares de várias naturezas mantidas na duração – do caminho por qual a estratégia quer atingir um dos seus rumos que ela se fixe num espaço-tempo dado, espaço-tempo decorrentes dos objetivos políticos."[4] (Jean Baechler. Artigo "Guerre et Paix". Dicionário do pensamento sociológico. 2005. Tradução nossa.)

Na forma, ele introduziu três princípios que ditam a prática da guerra: a oposição entre a aniquilação e a atrição; a alternância temporal da ofensiva e da defensiva; e o movimento entre a posição – postura estática – e a manobra – postura dinâmica. Desta forma, Svechin definiu uma linha de execução estratégica.

Estruturando o seu pensamento desta maneira, Svechin religou todos os ramos da guerra, tornando os objetivos como elementos fundamentais: a estratégia mostra o caminho e a meta, e os avanços operacionais são feitos por meio da multiplicidade dos passos relevantes executados pela tática (Olsen, 2010). Por isso, o General russo decompõe uma operação ao redor de uma linha de execução estratégica e um planejamento em quatro etapas: o enunciado do objetivo; a determinação da forma da operação por decomposição em missões para cada componente; a identificação dos requisitos geográficos e materiais; e a divisão da operação por fases, cujo apenas a primeira é detalhada com precisão.

Essa concepção inovadora estabelecendo um nível entre os níveis estratégico e tático se tornou uma referência essencial no processo moderno de planejamento, na delegação da tomada de decisão e na utilização dos combates no âmbito da guerra (Bihan, 2023).

2.1.2 Distinção entre *xadrez* e o *go*.

Nos anos 1920, as capacidades do Exército Vermelho estavam enfraquecidas. Não permitiriam resistir em caso de confronto com o bloco ocidental. Assim, a situação política, econômica e militar da União das Repúblicas Socialistas

[4] « On peut définir l'opération comme la matérialisation – sous la forme d'une combinaison d'activités militaires de natures variées entretenues dans la durée – du cheminement par lequel la stratégie entend parvenir à l'un des buts qu'elle se fixe dans un espace-temps donné, espace-temps qui dépend des buts politiques poursuivis. »

Soviéticas (URSS) – passando a denominar Rússia a partir de 1991 –, impulsionou o pensamento estratégico para conceber novas maneiras de dirigir os combates de forma mais eficaz e eficiente. A arte operacional de Svechin é um fruto dessa onda de reflexão. No entanto, a arte operacional não é uma doutrina universal. Ela integra também os valores fundamentais próprio de um país. Nesse escopo, a ferramenta de Svechin estabelece tanto princípios intangíveis (Bihan, 2023) quanto um raciocínio situacional. Alinhado com o trabalho de Clausewitz e a cultura soviética, a arte operacional surge como uma visão mais contemporânea e incisiva.

Este salto conceitual é uma verdadeira ruptura. Ela abriu a transição entre dois modelos de estrategistas, ou seja, dois modos para empregar a violência, a fim de atingir o rumo da guerra. Em particular, esses modelos se opõem em termo de espaço, de gestão do tempo e de compreensão dos objetivos. Para entender melhor esta ruptura, temos que mergulhar no espírito de um jogador de xadrez, que se joga com peças, que decidiu aprender o jogo de *go*, que se joga com pedras (Saucin, 2004).

Em primeiro lugar, essa transição se releva na escala espacial (Saucin, 2004). De uma concentração de forças para liderar a batalha decisiva, comum ao jogo de xadrez, os combates se tornam de maneira mais difusa, no jogo de go, onde o estrategista quer concentrar suas forças em vários combates bem escolhidos e localizados, e, sobretudo, em um espectro amplo incluindo a complementaridade das ações em todas as dimensões físicas – ou seja, nos cinco meios e dois campos de confrontação[5] (Burkhard, 2021). Assim, não só o *go* tem um tabuleiro – o *goban* – maior do que o de xadrez, mas também várias batalhas locais ocorrem no *goban*, chegando-se à vitória sem necessariamente uma batalha decisiva (Millequant, 2021). Do mesmo modo, a arte operacional abala o conceito da batalha decisiva localizada do Almirante americano Alfred T. Mahan (Penisson, 2019, p. 274) e o da concentração da maior massa de forças num esforço combinado no ponto decisivo de Jomini (Penisson, 2019, p. 25).

Também, no *goban*, as pedras não são posicionadas nos quadrados, mas nas intersecções das linhas. No espírito do jogo, isso significa que a geografia tem que ser percebida mais como um conjunto de linhas de força que espaços terrestres,

[5] Conforme a estratégia francesa, existe cinco meios de confrontação (terra, mar, ar, espaço e ciberespaço) e dois campos de confrontação (eletromagnético e informacional).

marítimos e aéreos sem vínculos entre eles. Essa visão introduz a percepção conjunta necessária ao estrategista. Svechin pensou e se apropriou do ar e do mar na manobra global (Bihan, 2023, p. 278).

Em segundo lugar, a transição exprime uma outra visão da gestão do tempo (Saucin, 2004). No início do jogo de Xadrez, o tabuleiro já está configurado com todas as peças disponíveis, organizadas de maneira semelhante. O jogo representa um confronto direto e imediato, enfatizando apenas a manobra no curto prazo. Ao contrário, o jogo de *go* se divide em três partes. A fase inicial – o *fuseki* – corresponde a um *goban* vazio onde os jogadores implantam suas primeiras pedras, criando zonas de influência e fortalecendo as bases de retaguarda (Millequant, 2021). A fase intermediária – o *chuban* – vê-se aparecer no *goban* pontos inexpugnáveis, várias frentes de batalha e zonas-tampão. Na terceira e última fase – o *yose* –, se desenha a vitória global (Saucin, 2004). Por definição, ela não é total e absoluta na totalidade das batalhas e da frente. Os sucessos em pontos estratégicos, bem escolhidos pelo estrategista, se tornam determinantes para o resultado geral, apesar das derrotas menores, à periferia dos objetivos reais (Millequant, 2021).

Essa visão de longo prazo, em fases, no jogo de *go* representa perfeitamente o pensamento da arte operacional de Svechin, na qual ele concebia o planejamento como um processo em quatro etapas: enunciar o objetivo, determinar o forma a decompondo em missões para cada componente, identificar pré-requisitos geográficos e materiais, e dividir a operação em fases ao longo do tempo (Bihan, 2023, p. 163). Ele promovia a aplicação da sua teoria ao contexto da União soviética[6], considerando que, em caso de conflito contra o ocidente, a União Soviética tem que trocar espaço contra tempo a fim de mobilizar o seu campo de poder, ou seja, as forças de trabalho. Isso mostra a altura do pensamento do General russo, e a sua crença em usar a fonte quase inesgotável de recursos de seu país ao longo do tempo, em vez de precipitar uma guerra com recursos limitados.

[6] No início dos anos 1930, Svechin é convencido que a URSS deve adotar uma postura defensiva em relação ao Ocidente, não estando pronta para enfrentar uma guerra direta contra ela. Ele promovia um fortalecimento progressivo antes de ser capaz de vencer. Sua visão foi suplantada pela de seu rival Tukhachevsky, mais conforme ao espírito stalinista que não podia revelar nenhuma fraqueza, mesmo passageira. (Bihan, 2023)

Por fim, a arte operacional de Svechin é uma evolução na construção da estratégia decorrentes dos objetivos da guerra. Assim, a partir de objetivos positivos e negativos fixados nas diferentes partes do tabuleiro, o jogo de *go* exclui a lógica de aniquilação de xadrez – um conceito teórico possível, mas pouco aplicável por causa dos riscos fortes e inaceitáveis que ela provoca (Bihan, 2023). Ele foca na luta entre estrategistas em vez de entre táticos. O jogo de *go* é mais coerente com a lógica de atrição, com opções de ajustar o nível de intensidade nas posições fracas do adversário e de controlar, tanto quanto possível, o nível de fricção[7] (Millequant, 2021).

Por outro lado, o estrategista não pode reduzir as peças jogadas ao seu valor intrínseco - como poderia ser feito no xadrez. Ao contrário, como no jogo de *go*, ele valoriza as pedras pela posição, pela ameaça que representam para o adversário e pelo referencial geoestratégico dele.

Além disso, é importante destacar que o fim de um jogo de go ocorre com a aceitação para um dos estrategistas da sua derrota. Isso é relevante com o princípio segundo o qual a vitória existe somente quando reconhecida pelo adversário, como Clausewitz explicou na sua análise da campanha de Napoleão na Rússia em 1812 (Bihan, 2023, p. 60).

A arte operacional de Svechin, sob uma perspectiva nova, transcendeu o trabalho de Clausewitz e revolucionou a essência da estratégia em relação aos objetivos da guerra, e aos princípios para os atingir, no tempo e no espaço.

2.1.3 Mudança de paradigma de conflitualidade.

Desde o fim da guerra fria, a grelha de leitura do mundo estava focada no contínuo “paz-crise-guerra”. Essa interpretação não via os conflitos com uma dinâmica global, mas com uma escala bem marcada das interações interestatais. Os dividendos da paz e esse ponto de vista simplista das interações humanas levaram os países a acreditar que a violência podia se manter longe graças ao quadro de segurança global e a afirmação intangível do direito internacional.

[7] No pensamento de Clausewitz, a fricção é uma noção fundamental representando uma grande variedade de fatores imprevisíveis e perturbadores que influenciam a condução da guerra conforme os planos, e de onde nasce a incerteza.

No entanto, com a explosão da Internet e seu ecossistema social introduzido pela sua versão 2.0[8], foi imprescindível reconhecer o aparecimento de novos espaços comuns, pouco regulamentados e controlados. Reveladas tragicamente nas ruínas do World Trade Center após o dia 11 de setembro 2001, essas novas zonas cinzentas estavam se tornando propícias aos posicionamentos agressivos e, sobretudo, uma nova fonte inesgotável de incerteza (Boyer, 2020). As forças armadas já estavam atrasadas frente a enorme onda que se preparava para impor uma nova relação de forças no cenário global, abalando a definição mesma da paz.

> « A paz não poderia ser definida como um estado marcado pela ausência de conflitos, porque esse estado não existe e não pode existir, mas como resolver os conflitos humanos sem recorrer à violência. »[9] (Bihan, 2023, p. 110, Tradução nossa.)

Em 2021, o novo Chefe do Estado-Maior das forças armadas francesas (CEMA), o General Thierry Burkhard, publicou a sua visão estratégica. Nesse documento, o CEMA considerou como imprescindível perceber a mudança profunda do paradigma estratégico moderno. Segundo o presidente francês Emmanuel Macron,[10] “a guerra não é mais declarada, é travada em silêncio, insidiosamente, ela é híbrida” (Macron, 2023)[11]. Como um eco a essa declaração feita durante a apresentação do projeto de lei de programação militar 2024-2030, no dia 20 de janeiro 2023, o CEMA anunciou a sua percepção do padrão atual da conflitualidade. Assim, o novo tríptico em qual as forças francesas se incluem está agora definido como sendo “**competição**-**contestação**-**confrontação**” (Burkhard, 2021).

A **competição** é o curso normal da expressão do poder (Burkhard, 2021). Assemelhando-se a uma "guerra antes da guerra", ela ocorre em todos os domínios: diplomático, informacional, militar, econômico, jurídico, tecnológico, industrial e cultural. Em particular, nos espaços comuns caracterizados por uma liberdade de

---

[8] Internet 2.0 desenvolveu as plataformas web onde os usuários não são apenas consumidores de conteúdo, mas também contribuem ativamente, criando conteúdo, compartilhando informações e interagindo por meio de fóruns , blogs e outros serviços online precursores das mídias sociais.

[9] « La paix ne saurait être définie comme un état marqué par l’absence de conflits, car cet état n’existe pas et ne peut pas exister, mais comme la résolution des conflits humains sans recours à la violence. »

[10] Discurso as forças armadas francesas 2023.

[11] « La guerre ne se déclare plus, elle se mène à bas bruit, insidieusement, elle est hybride. »

ação quase sem limite; um direito internacional perfectível e facilmente contornável; e uma dificuldade de imputar uma ação maliciosa.

A **contestação** é o período “apenas antes” da guerra (Burkhard, 2021). Nesta fase, é essencial agir com alta reatividade e com habilidades adequadas para reduzir a incerteza e evitar a imposição de fatos consumados. Além disso, o ponto-chave é entender as intenções dos atores, a fim de reafirmar os objetivos nacionais, desencorajar o adversário e assegurar o retorno ao respeito pelo direito.

Quando um ator persiste a usar a força para alcançar seus objetivos, isso pode levar ao **confronto.** Neste ponto, o objetivo é subjugar o adversário. As forças devem estar prontas a antecipar a escalada do confronto, assim que os sinais fracos aparecem e em qualquer espaço de conflitualidade (Burkhard, 2021).

Desta forma, o novo paradigma de conflitualidade francês traz um novo fôlego à reflexão estratégica, operacional e tática. Ele coloca em perspectiva os meios e campos de confrontação com uma conflitualidade movente, onde um conflito pode ser muito intensivo, mesmo abaixo do limiar da confrontação. Esse novo panorama da defesa redinamiza a teoria da “abordagem indireta”, ou seja, o uso de fatores psicológicos na guerra, elaborada por o inglês Sir Basil H. Liddell Hart no seu livro “*Estratégia*” em 1954.

2.2 QUADRO OPERACIONAL: UM ALINHAMENTO GLOBAL

2.2.1 Importância da ambição político-estratégica

Quando Clausewitz escreve que a guerra é a continuação da política por outros meios (Da Guerra, 2014, p. 45), ele destaca o vínculo fundamental entre a guerra e os objetivos superiores do Estado. Assim, atrás desses objetivos que desenham um potencial futuro para uma Nação, sempre se esconde uma vontade para expressar seu poder frente aos seus competidores, considerando que no caso da guerra, essa expressão do poder se tornou violenta (Bihan, 2023). Liddell Hart, militar e historiador inglês, nomeou essa vontade a Grande Estratégia.

> « O papel da grande estratégia consiste em coordenar e dirigir todos os recursos da nação ou de uma coalizão, a fim de atingir o objeto político da

> guerra, objetivo definido pela política fundamental. » [12] (Liddell Hart. Stratégie, p. 394, Tradução nossa)

Clausewitz coloca a guerra no centro de uma trindade[13] representada pela a tríplice hélice do governo, da força armada e do povo. Da sua vez, Hart sugere que a arte operacional, por ser naturalmente dependente da Grande Estratégia, é condicionada não apenas pelos objetivos políticos, mas também pelos recursos investidos no longo prazo. Na realidade, essa Grande Estratégia define a ambição político-estratégica nacional, por peio do qual um Estado estabelece um futuro desejável a seu povo num mundo volátil, incerto, complexo e ambíguo. No contexto da defesa e da segurança, essa ambição se materializa notavelmente por meio de uma hierarquia das normas documentárias específica.

Por exemplo, no Brasil, essa ambição é traçada pela Política Nacional de Defesa (PND), a Estratégia Nacional de Defesa (END) e o Livro Branco da Defesa Nacional (LBDN). Essa visão política, acionada pelo plano plurianual (PPA), se completa no plano civil, com perspectivas industriais e científicas – a tríplice hélice –, e no plano militar, com documentos complementares de todos os níveis de comando – Política Marítima Nacional (PMN), Plano Estratégico da Marinha 2040 (PEM-2040), doutrinas e ordens.

De maneira semelhante, a ambição da França se apoia sobre um Livro Branco de Defesa e de Segurança Nacional (LBDSN 2013), uma Revista Nacional Estratégica (RNS 2022) e uma Lei de Programação Militar Plurianual (LPM 2024-2030).

Essa documentação fixa os princípios gerais e particulares, atuais e futuros. Ela representa uma outra matéria-prima da arte operacional, que deve relevar o desafio da combinação dos recursos e das ferramentas de poder nacional para se impor, desde o tempo da competição até o conflito violento.

---

[12] “Le rôle de la grande stratégie consiste en effet à coordonner et diriger toutes les ressources de la nation ou d’une coalition afin d’atteindre l’objet politique de la guerre, but défini par la politique fondamentale.“

[13] Trindade formada pelo povo, pelo general (e sua força armada) e o governo (Da guerra, Livro 1, Cap. 28, p. 47).

2.2.2 O planejamento: etapa-chave entre antecipação e a ação

Para se alinhar com a ambição político-estratégica nacional, a estratégia militar tem que explorar os recursos recebidos com eficiência, ou seja, tomar medidas coerentes e pertinentes para possuir capacidades com um alto nível de desempenho e de prontidão. Esse desafio militar de forma industrial, humano e institucional[14] marca o objetivo permanente de estruturar o quadro físico – materiais e homens – e moral – ideal e determinação – para conduzir missões no conjunto do espectro da conflitualidade (MINARM, 2022).

Isso se focaliza no ponto comum da construção das capacidades militares e de concepção de cenários internacionais, continentais e nacionais: o tempo. Longo, real, favorável ou útil, o tempo possui múltiplas características. Nas suas aplicações militares diretas, o estrategista está numa projeção perpétua: a antecipação.

Na doutrina francesa, a **antecipação** é um processo de alto nível e ascendente para informar os decisores. Ela é dividida em dois conceitos complementares: a **prospectiva** e a **antecipação estratégica**[15].

A partir de fenômenos emergentes ou observáveis, a **prospectiva** é uma ferramenta de apoio à decisão no horizonte longo, geralmente de vinte a trinta anos.

Um nível embaixo, a **antecipação estratégica** é um processo focado no médio prazo, ou seja, nos próximos dois ou três anos (MINARM, 2022). Seu papel é reduzir a incerteza sobre as evoluções do ambiente internacional, em particular, no entorno estratégico. No ponta de vista militar, esse exercício mental permite sincronizar os programas, gerenciar os fluxos de recursos humanos e orientar os captores de inteligência.

Do outro lado da linha do tempo, os engajamentos operacionais, ou seja, as operações e as missões, são levantadas no presente e na realidade tática. Eles resultam da tomada de decisão e se incluem no processo descendente de modelagem efetiva do mundo real (MINARM, 2022).

Dobradiça entre a antecipação e os engajamentos operacionais, o planejamento é uma etapa-chave. Colaborativo e multidisciplinar, o planejamento é tradicionalmente o processo de construção de uma operação militar resultante de

[14] No Brasil, esse desafio militar é apoiado para o círculo virtuoso da Tríplice Hélice.
[15] Definições inspiradas do relatório de informação n° 585 (2010-2011) da comissão das relações exteriores e defesa do senado francês. (Robert del Picchia, 2011)

uma decisão política, frente a um problema complexo. Também, a fim de se beneficiar de uma visão tanto global quanto precisa, sua forma é **paralela** e **sequencial**.

O trabalho **paralelo** faz com que cada nível de comando – estratégico, operacional e tático – possui recursos e prerrogativas para o entendimento das suas partes dos objetivos da operação e para a elaboração de respostas coerentes com suas capacidades e suas condições de emprego (MINARM, 2022).

O trabalho **sequencial** visa cortar a complexidade do problema para uma melhor compreensão parcial, até a reconstrução de um plano comum a todos os níveis, tomando em conta essa complexidade, formando uma estrutura eficaz de comando e controle, e oferecendo uma opção militar – um curso de ação e uma sequência temporal – a mais compatível com os objetivos do nível político .

Neste ponto, vale destacar que o planejamento não é só um processo usado antes de uma crise, mas também uma ferramenta que faz parte da condução durante a crise – em particular, por meio da seção de planejamento D-5 do Estado-Maior.

2.2.3 O desafio da inteligência.

No seu papel de decidir as opções militares relevantes para enfrentar um problema complexo, o planejamento integra necessariamente um objetivo imprescindível: a redução da incerteza, também chamada a névoa da guerra.

> "A dificuldade de *ver com precisão* constitui uma das maiores fricções na guerra."[16] (Clausewitz, Da guerra, 2014, Capítulo VI. p. 89, Tradução nossa)

Considerando a incerteza como uma fricção, Clausewitz vê a sua gestão como um desafio essencial e permanente. Por um lado, ela gera um enfraquecimento da intensidade da guerra (Dabila, 2013), levando a superestimar as forças do adversário e a protelar nossa ação. Por outro lado, ela complica as decisões criando riscos operacionais e táticos inaceitáveis sem mitigação.

A ferramenta crucial para lutar contra a incerteza é a inteligência. Na sua doutrina de atividade de inteligência, a Agência Brasileira de Inteligência (ABIN) a

[16] « La difficulté de *voir juste* constitue une des plus grandes frictions à la guerre. »

define como um processo integrado de coleta, cruzamento e análise de dados e, a partir delas, de produção e disseminação de conhecimentos visando à redução de vulnerabilidades, à neutralização de ameaças e à identificação de oportunidades. No planejamento, ela contribui para a elaboração das opções militares como processos-chave da tomada de decisão e da seleção de alvos.

No entanto, a inteligência é uma atividade permanente – na globalidade do novo paradigma da conflitualidade – e constitui os alicerces da autonomia de apreciação da situação, em qualquer nível de comando, para a orientação e a animação das suas capacidades (RNS, 2022).

Acompanhando o processo de planejamento e de execução operacional, a inteligência se estende sobre várias origens, como: eletrônica (ELINT), sistemas de comunicação (COMINT), informações abertas (OSINT), geográfica (GEOINT), humana (HUMINT) ou imagem (IMINT)[17]. Também, cada conhecimento tem que ser avaliado com a confiabilidade da fonte, a veracidade da informação e a duração de validade. Vale destacar que o processo de inteligência concerna não apenas o adversário, mas também as forças amigas ou neutras. Assim, todas as organizações no entorno da operação, que podem ter um impacto na nossa força ou aparecer como uma alavanca para a missão, podem ser de interesse.

O avanço tecnológico, impulsionado pela emergência do digital, pelo crescimento das capacidades espaciais e pela Internet, faz com que grande parte da inteligência de interesse militar atual se tornou técnica. Sem ignorar a importância das técnicas humanas de coleta – cujo meta é muitas vezes tirar informação sobre falhas das tecnologias adversária –, a inteligência técnica é o pivô dessa atividade estratégica. Existe uma forma de paradoxo da inteligência técnica: quanto mais ela é desenvolvida por instituições estatais, mais aparecem o tamanho das zonas cinzentas que se criaram no espaço digital, e mais medimos a distância que nos separa da dissipação da névoa da guerra. Instituições têm que enfrentar o desafio do processamento em massa (Boyer, 2020), onde os dados de interesse estão agora afogados em um volume não tratável pelo ser humano e, muitas vezes, criptografados.

[17] HUMINT : Human Intelligence; IMINT : Imagery Intelligence; OSINT : Open Source Intelligence; COMINT : Communications Intelligence; ELINT : Electronic Intelligence; GEOINT : Geografic Intelligence.

No final, a inteligência, reduzindo apenas a incerteza em qualquer nível de decisão militar, é apenas uma revelação da distância que nos separa da realidade absoluta. Na era da informação, essa tomada de consciência do tamanho da névoa da guerra leva os estrategistas a concluir, como o filósofo Sócrates, que “sei que nada sei”. Isso o empurra para entrar no campo da arte, ou seja, enfim expressar suas vontades e mexer suas qualidades de racionalidade e de intuição para ganhar a guerra.

3 O CIBERESPACO: A ESTRUTURA EM CAMADA DESAFIADORA

Na sua estratégia de ciberdefesa de 2011[18], a França definiu o ciberespaço como o espaço **comum** de comunicação constituído por uma interconexão mundial de equipamentos de tratamento numéricos. Na doutrina militar de defesa cibernética brasileira (Ministério da Defesa, 2023), este espaço é virtual e chama a atenção sobre o procedimento e a armazenagem das informações digitais. Nesse ponto, vale destacar a composição do ciberespaço em três camadas (Boyer. 2020). A camada física abrange os meios físicos da rede, não só cabos de cobre ou fibra ótica, terrestres ou submarinos, mas também as ondas radioelétricas do terreno até o espaço extra-atmosférico. A camada lógica, por sua vez, junta os protocolos de comunicação, de roteamento e de qualidade de serviço, assim que o conjunto dos softwares que permite a exploração dos sistemas de forma simples e inteligível. A última camada é cognitiva (ou social), ou seja, ela dá o acesso aos dois primeiros níveis da pirâmide cognitiva individual[19] e permite o contato direto entre seres humanos.

Nesse sentido, o ciberespaço se divide em duas áreas diferentes: as duas primeiras camadas constituem o ciberespaço técnico e a terceira camada representa a parte ciber do campo informacional. No meio da segunda década do século XXI, o

[18] https://cyber.gouv.fr/publications/la-strategie-de-la-france-en-matiere-de-cyberdefense-et-cybersecurite-0

[19] Esse modelo piramidal consiste numa integração progressiva dos dados disponíveis em informações, elas mesmas integradas no plano de conhecimento, antes de se tornar mais tarde uma faculdade de entender, então de adaptar-se (inteligência), e, no final, de constituir uma consciência, a faculdade de sentir e pensar.

ciberespaço, como outros espaços comuns (mar, ar, espaço), passaram a ser objeto de uma competição de poder cada dia mais forte (Boyer, 2020). Essa parte detalha, para cada um, as características e desafios próprias. Ela destacará também o caráter permanente desses novos ambientes com ilustrações operacionais recentes.

3.1 O ciberespaço técnico

3.1.1 Características do meio

O ciberespaço técnico é constituído do seu suporte físico e de uma parte lógica, a fim de criar condições de estabelecer comunicações de dados e informações entre pessoas, entre máquinas ou entre uma pessoa e uma máquina. Suas características são de três ordens (Marangé, 2021).

Em primeiro lugar, o ciberespaço técnico se apoia sobre uma arquitetura física. Assim, mesmo se os serviços aparecem como desmaterializados e virtuais, vale ressaltar que cada dado armazenado na nuvem (Cloud) tem uma realidade física em um centro de dados em algum lugar no mundo. Assim, um arquivo transmitido num e-mail ou em um aplicativo de mensagens instantâneas, existe objetivamente em componentes eletrônicos, consumindo energia elétrica e uma largura de banda por sua troca. Essa característica leva o dado a transitar de nossos celulares até o fundo dos oceanos e os satélites bem acima de tudo (MINARM, 2019).

Em segundo lugar, ele se caracteriza por sua permanência e sua instantaneidade. Essas propriedades constituem uma ruptura da barreira do espaço e do tempo, largamente considerada como uma base à emergência do mundo globalizado, tanto de suas oportunidades, quanto de suas ameaças. Assim, o ciberespaço técnico oferece um encurtamento do espaço, permitindo atuar do outro lado do mundo em alguns segundos apenas. Da mesma forma, criou uma contração do tempo nos seus dois sentidos, ou seja, tanto no ritmo e na quantidade de ações nas redes, como a duração necessária para as executar (MINARM, 2019).

Em terceiro lugar, ele se caracteriza por sua versatilidade, especialmente em termo de ausência de fronteiras, de anonimidade e da heterogeneidade da concepção global, inclusive a de centro de dados de armazenamento. Assim, as oportunidades ainda crescentes de flexibilidade da rede para criar ou acessar aos

serviços está balanceada pelas ameaças tanto técnicas e ambientais, quanto humanas. Essa versatilidade é ao ciberespaço o que as fricções são no campo de batalha, uma caraterística que permite a um adversário exprimir sua criatividade (MINARM, 2019).

Alicerces do mundo globalizado enaltecendo as oportunidades de trocas entre seres humanos, o ciberespaço traz de maneira intrínseca com ele os riscos e ameaças [20] (Marangé, 2021). Assim, ao aproximar os países competidores estratégicos e exacerbar as vontades de poder num espaço comum, tornou possível lutar com armas iguais e riscos minimizados de ser designado como o responsável pelo ato.

3.1.2 Princípio da postura permanente de cibersegurança

Para instituições nacionais, as características do ciberespaço técnico impõem necessidades permanentes de proteção e de defesa. Nessa perspectiva, três características principais são definidas para identificar e analisar os riscos e os danos sobre os valores digitais, a fim de antecipar as medidas adequadas: a confidencialidade, a integridade e a disponibilidade (Marangé, 2021).

A confidencialidade significa o acesso às informações só por pessoas autorizadas, dominando os procedimentos para as gerenciar e tendo consciência da sua natureza sigilosa. A integridade especifica a qualidade dessas informações, considerando que elas não foram alteradas de maneira ilegítima. A disponibilidade significa a capacidade de acessar às informações em qualquer tempo que necessita uma consulta. (SGDSN, 2004)

Por um lado, a ciberproteção é uma tarefa que consiste em construir sistemas, conectados ou não, de forma segura tomando em consideração todos os aspectos ambientais internos e externos. Sejam pessoas, instalações físicas, criptografia dos dados e dos canais de comunicação ou computadores, tudo deve ser monitorado ao longo do ciclo de vida de um sistema de informação e de comunicação. Por definição, a ciberproteção é um ciclo contínuo e transversal, como um arquiteto melhorando constantemente a segurança intrínseca de uma fortaleza, ou seja, implementada no edifício, em relações com as times de defesa – que

[20] Na doutrina francesa, os riscos se diferenciam das ameaças: ameaças são associados a eventos internos ou externos tendo como origem uma vontade humana.

possuem seus próprios ferramentas complementares – e ao serviço de uma abordagem global dos riscos e ameaças (JORF, 2017).

Por outro lado, a ciberdefesa adota um ponto de vista operacional, de natureza permanente. Ela usa não só os dispositivos nativos dentro dos sistemas concebidos com um alto nível de ciberproteção, mas também ferramentas específicas de detecção, de análise e de resposta frente um caso não conforme, em particular durante ataques cibernéticos. Essa capacidade complementar da ciberproteção necessita um saber-fazer muito especializado, notavelmente para criar uma base técnica de referência em qual os elementos técnicos devem servir a conhecer as ameaças no rumo da detecção e da imputação[21] (JORF, 2017).

Além disso, para garantir a eficácia das funções de proteção e de defesa cibernética, a palavra-chave é a permanência. Essa necessidade concilia ambas funções em uma postura tanto estática quanto dinâmica. Por um lado, a parte estática possui capacidades de detecção enriquecidos pela função ciber da inteligência e pelo conhecimento preciso do uso dos sistemas. Ela estabelece uma **escala de risco e ameaça**, melhorando de maneira contínua a robustez dos sistemas e justificando as previsões de eventos de origem cibernética, inclusive ataque intencionais de nível estatal (Marangé, 2021).

Por outro lado, a parte dinâmica possui capacidades e recursos dedicados, a fim de limitar o impacto de eventos cibernéticos e preservar os serviços e os dados. Estabelecendo um estado de alerta e os procedimentos ativos de resposta, ela se torna rapidamente uma função crítica para a compreensão de um evento cibernético, em qualquer nível da cadeia de comando e controle.

3.1.3 Desafios do planejamento de operações no ciberespaço

Na sua parte técnica, o ciberespaço se construiu de maneira heterogênea com sistemas autônomos interconectados no mundo inteiro (Schafer, 2020). A velocidade de desenvolvimento de Internet foi tão rápido e intensivo que não é mais possível mapear nem a rede global, nem o funcionamento local. A complexidade de implantação física, a multiplicidade dos fluxos criaram zonas cinzentas, ou seja,

[21] A imputação é o fato de ser em medida de associar um evento cibernético com uma ameaça (APT, *Advanced persistente threat*), estabelecendo uma relação entre os dados técnicos coletados durante o evento e os dados conhecidos do grupo responsável desse evento.

micropartes da rede onde não há regulação. Elas constituem santuários invisíveis, fulcro das vontades belicistas transpostas no plano digital (Boyer, 2020). Como a execução de uma operação alternando ataque e defesa, as instituições militares devem constituir um portfólio de capacidades tanto ofensiva quanto defensivas. Esses desafios concernam o domínio dos dados, o tempo longo para desenvolver um arsenal ofensivo e a ruptura necessária na implementação de novas técnicas defensivas.

No pensamento militar francês (RNS, 2022), a superioridade técnica no ciberespaço é buscada para fortalecer a eficácia das operações, por meio da capacidade de controlar e proteger os dados da cadeia de comando e controle. Assim, dados representam recursos estratégicos, base da informação e do conhecimento[19], que devem ser explorados num escopo de “saber-fazer” técnicos avançados, de “saber-ser” individuais e coletivos adequados e de uma legislação nacional coerente. Assim, a soberania digital tem que ser perguntada no momento da escolha de localizar fisicamente dados em *datacenters* nacionais ou no exterior (disponibilidade), e de proteger sistemas nacionais com criptografia fiável (integridade e confidencialidade). Esse desafio reside em estabelecer infraestrutura soberana e sistemas robustos de processamento abrangendo técnicas de *Big Data*, de virtualização e boas práticas (Marangé, 2021).

No ponto de vista militar, obter efeitos por meio de ações cibernéticas – dentro do ciberespaço, contra ou a partir dele – se prepara de longo prazo. Por definição, isso supõe que os sistemas do adversário foram mapeados, incluindo a coleta de informações técnicas e a identificação de vulnerabilidades efetivas ou potenciais. Processo intrinsecamente longo e complexo, a construção de um arsenal ciberofensivo envolve não apenas a coleta de inteligência de origem e de interesse cibernética, mas também o desenvolvimento de ferramentas e técnicas para explorar as falhas. Vale ressaltar que uma arma cibernética é por natureza um “rifle de tiro ·único” (Marangé, 2021), porque seu uso revela geralmente as falhas exploradas aos olhos do adversário. Além disso, manter este arsenal com um alto nível de prontidão, para ser empregado em um ambiente constantemente alterado, necessita tempo, recursos e competências raras. Em suma, o desenvolvimento de capacidades ofensivas no ciberespaço requer um planejamento extensivo e

meticuloso que precede o planejamento por si só. Isso significa que essas capacidades têm que ser pensadas desde a antecipação estratégica.

Enfim, o terceiro desafio da integração de processos defensivos no planejamento militar em qualquer nível de comando e controle. Assim, prever como fazer frente e confrontar um adversário tecnologicamente mais avançado tem que levar os estados-maiores ao pensamento de ciberdefesa. Conhecer as suas próprias fraquezas, possuir planos de resiliência para a continuidade da atividade e ser, em grande medida, capaz de adaptar dinamicamente seu nível de proteção, é vital desde o estado da competição. O uso de tecnologias avançadas, como a inteligência artificial (IA), pode levar à transformação de uma postura cibernética defensiva em uma abordagem mais proativa. Em breve, as ferramentas poderiam implementar novas tecnologias para uma abordagem preditiva, visando a neutralização das falhas e das ameaças antes que elas se concretizem (Marangé, 2021).

3.1.4 O episódio do início da guerra na Ucrânia

Para ilustrar as características e os desafios das dimensões físicas e lógicas do ciberespaço, a operação que liderou a Rússia contra a Ucrânia em fevereiro 2022 é particularmente pertinente. Assim, pouco tempo antes da invasão terrestre da Ucrânia pela Rússia no dia de 24 de fevereiro de 2022, uma série de ataques cibernéticos significativos foram lançados contra a Ucrânia no dia 23 de fevereiro. Estes ataques tinham por objetivos desorganizar as comunicações e infraestruturas críticas do país. Pela primeira vez na história dos conflitos, um ataque cibernético iniciou as hostilidades militares, prova que o ciberespaço já se apresenta como um amplificador de efeitos tanto antes, quanto durante uma operação. Essa operação cibernética da Rússia procurou explorar vários métodos com foco no descrédito de Kiev, em prol do enfraquecimento do moral ucraniano e de seus sistemas de informação e comunicação civis ou militares.

O primeiro tipo de ataque foi o de negação de serviço, nomeado **ataques DDoS (*Distributed Denial of Service*),** tendo o objetivo de sobrecarregar plataformas técnicas de armazenagem, paralisar os serviços públicos e de semear pânico dentre da população ((Rid, 2013). Geralmente considerado como uma linha

de ação barata e conveniente numa relação do fraco contra o forte, a Rússia alcançou notavelmente sites ministeriais e bancários ucranianos.

O segundo tipo de ataque usou *malwares* destrutivos da família dos "*wiper*", tendo como objetivo destruir sistemas de computador. Alvejando os dados, esse malware foi projetado para corromper e apagar informações nos computadores infectados. Seja nas infraestruturas críticas como instituições financeiras ou agências governamentais, ou nas entidades comerciais ou pessoas, esses ataques tinham alvos de alto valor – os dados – cuja a perda, quando ela é definitiva, pode desestabilizar fortemente as organizações, assim como a credibilidade do governo e das instituições (RNS, 2022).

Enfim, o terceiro tipo de ataque utilizado pela Rússia foi de natureza mais poderosa. Essa categoria juntou verdadeiras armas cibernéticas, desenvolvidas de propósito para atingir um alvo preciso e de alto valor ou complexidade. Esse armamento cibernético impõe requisitos amplos tanto em termo de competências técnicas, de instalações e de inteligência, quanto de tempo de desenvolvimento – de alguns meses até vários anos – e de apoio financeiro, ou seja demanda um intenção hostil inicial, uma preparação específica e uma manutenção constante, todas de longo prazo. Assim, uma hora antes da invasão da Ucrânia, esse tipo de armas foi usado contra o sistema de satélites Ka-Sat da empresa Viasat, provocando uma ruptura parcial das comunicações no comando e controle militar ucraniano. A partir de evidências técnicas, este ataque foi atribuída de maneira certa à Rússia pela União Europeia (Josep Borell).

Vale destacar que os especialistas cibernéticos lhe chamam "arma de um só tiro". Especificidade dessas armas cibernéticas que buscam explorar uma falha de concepção do sistema (falha "*dia-zero*"), o seu uso é único e tem que provocar um máximo de danos antes que a falha seja corrigida.

3.2 O campo informacional

3.2.1 Características do campo informacional

A cada minuto na Internet em 2024, os usuários enviam mais de 40 milhões de mensagens Whatsapp, escrevem 350 mil tweets, compartilham mais de 500

horas de vídeos no Youtube (GCS[22]). Além disso, o mundo se prepara para à conexão 5G, quinta geração de serviços móveis, que deverá dar um impulso exponencial à quantidade de informação gerada com uma nova explosão dos débitos, tornando realidade a Internet das coisas (IoC, ou *Internet of Things*, IoT), as inovações da inteligência artificial ou a desmaterialização total da vida social por meio de metaversos. Se o seu acesso já é quase generalizado, a informação é hoje ela-mesma o centro de uma contestação sem precedente nesse espaço modelado pelos grandes operadores do Internet (Boyer, 2020).

A primeira característica principal do campo informacional é a contração do tempo e do espaço (MINARM, 2021). Assim, a acessibilidade global, eliminando as barreiras geográficas, permite um acesso em tempo real e simultâneo a qualquer dado e o conhecimento de qualquer evento no mundo. A sensação de proximidade global apaga completamente a distância física, ou seja, facilita a colaboração e a troca de informações independentemente do fuso horário e, muitas vezes, sem filtro.

Uma segunda característica é a remanência das informações (MINARM, 2021), ou seja, a persistência dos dados e metadados (históricos de navegação, comportamento de navegação) por longos períodos. Mesmo apagado de um site, um conteúdo pode ter sido copiado, arquivado ou compartilhado em outros lugar, tornando a sua retirada praticamente impossível. A emergência de infraestruturas físicas dedicadas, de ambientes virtualizados e a extensão do efeito de rede permitiram o armazenamento e o tratamento de grandes quantidades de dados a um custo reduzido. Isso favoreceu também a criação de novos espaços cognitivos baseados nas audiências.

Enfim, vale ressaltar a grande liberdade individual no ciberespaço (MINARM, 2021). A interatividade de grande escala surgiu com a evolução do Web 2.0, a criação dos redes sociais e a explosão do número de objetos conectados. Favorizado pelo anonimato relativo e pelos mecanismos técnicos e jurídicos de proteção da privacidade, esse processo se revelou um vetor poderoso de expressão, tanto de opiniões, ideias e sentimentos, quanto da criatividade, da autonomia profissional ou da formação pessoal.

[22] GCS: *Government Communication Service* do Reino Unido.

Então, o campo informacional aparece como um espaço continuo, um traço direto, entre o aspecto técnico do ciberespaço e a área cognitiva dos usuários que se tornaram consumidores da informação. Em prol das teorias de retórica, de marketing e de venda, esse espaço é visto como uma nova terra de conquista (MINARM, 2021). Ele se tornou um campo virtual de batalha. Mudar as percepções, polarizar as mentes, alcançar e mobilizar as audiências-alvos são agora os novos objetivos de países que se tornam potências de desequilíbrio para se impor no escopo internacional. O campo informacional ofertado pela Internet é o seu novo campo de jogo, um jogo sério e perigoso para o modelo da democracia.

3.2.2 O desafio dos Estados democrático : ataques informacionais.

Em 1964, Marshall McLuhan introduziu a tecnologia como uma extensão de nós mesmos (McLuhan, 1964, p. 17), bem como o smartphone se transformou em uma extensão da mão e de nossa identidade digital. Assim, as pessoas têm deixado deliberadamente a tecnologia entrar em contato direto com a sua consciência. Nesse sentido, “o meio se tornou a mensagem”, ou seja, os objetos tecnológicos configuram e controlam a proporção e a forma das ações e associações humanas (McLuhan, 1964, p. 18). Isso desenhou um novo tipo de poder tangível na era da informação: o poder discursivo, capaz de introduzir, amplificar e manter narrativas, vistas, padrões ou valores, a fim de moldar o pensamento de alvos nos novos espaços de comunicação.

Na competição entre Estados, por natureza híbrida, ações no campo informacional têm um aspecto versátil e sorrateiro. Assim, esperando criar uma assimetria definitiva nas condições da competição, de um conflito ou de uma guerra, os ataques informacionais buscam ter um impacto direto num pilar da trindade de Clausewitz: as opiniões e as paixões do povo. Minar a vontade de competidores pela informação se tornou os novos objetivos de alguns países ou grupos maliciosos. Os novos métodos de sabotagem, espionagem e subversão (Rid. 2013) surgirem para engajar a luta contra, para e pela informação. Na luta contra as ingerências, eles aparecem tanto como um vetor de fragilização e de descredibilização do poder político, quanto como um desafio de soberania nacional para as democracias (Marangé, 2021).

Difícil de detectar e de combater, os ataques informacionais (*misinformation*, *desinformation* e *malinformation* [23]) fazem da desestabilização um fator de superioridade estratégica, tendo um alcance multiplicado pelas ferramentas digitais. A estratégia perseguida é, geralmente, a 360 graus, incluindo a diplomacia clássica, a polarização nas redes sociais, o uso de cadeias de televisão como proxy, o ingresso das diásporas emigradas e das redes criminais e a valorização de bens e práticas culturais (Marangé, 2021). Tirando benefícios das características do ciberespaço técnico, o mercado da influência passou estar a serviço de estratégias de poder desinibidas.

Se a guerra é, segundo Sun Tzu, a arte de enganar, o uso de ataques informacionais aumenta a confusão e o medo na população. Isso é também uma maneira artificial e poderosa de crescer a incerteza para os decisores, em qualquer estágio da conflitualidade, competição, contestação e confrontação. Numa perspectiva de defesa, a questão da proteção contra a seleção de alvos dentro da população nacional por competidores é crucial. Ela abre um campo de pesquisa dual (civil e militar) a fim de negar qualquer perda de iniciativa dos Estados, frente aos agentes desestabilizadores.

3.2.3 Planejamento operacional no campo informacional

Por analogia ao petróleo no século XX, os dados são o novo ouro preto da era da informação, ou seja, um recurso cuja exploração é uma fonte de desenvolvimento, de valor financeiro, de inovação e de vantagem competitiva. Além disso, desde a sua expansão, o ciberespaço se tornou um novo terreno de conquista política. As plataformas dos gigantes da Internet e da Web 2.0 criaram novas formas de expressão, de encontros e de rivalidades ideológicas. Nova fonte de poder, os dados têm uma diferença considerável face aos recursos fósseis: o ouro preto é agora renovável e inesgotável (Boyer, 2020).

No domínio da defesa e da segurança nacional, as forças armadas renovaram doutrinas, fazendo da superioridade informacional um fator operacional decisivo.

[23] No RESULT 2 toolkit, a *misinformation* é uma informação falsa compartilhada sem a intenção de enganar e induzir ao erro; a *desinformation* é uma informação falsa compartilhada com a intenção de enganar e induzir ao erro; a *malinformation* é o engano deliberada para distorcer o significado de informações verdadeiras

Visão mais ampla da guerra eletrônica e da inteligência (Marangé, 2021), ela aparece como o resultado da natureza híbrida dos conflitos, desde o estágio da competição e em qualquer nível de conflitualidade. No entanto, a quantidade de dados e de informações geradas na Internet está fora de controle dos governos. Atos maliciosos no campo informacional são hoje à origem de uma verdadeira intoxicação lenta, envenenando e polarizando, pouco a pouco, a esfera pública (MINARM, 2021). Nos seus planejamentos, as forças armadas fazem frente a três desafios críticos e concretos.

O primeiro desafio é a **cartografia a fim de detecção** – conceito de *information early-warning* (GCS RESULT2 toolkit, 2022) – de ataques informacionais. Geralmente uma função de defesa ativa na condução das operações, a detecção é um conjunto de três parâmetros definidos pelo estrategista. O primeiro é a cobertura, que define a escala das situações tática, operativa e estratégica. O segundo é a rapidez, que deve permitir a detecção em tempo real e um processamento imediato. O terceiro parâmetros é a precisão, cujo papel é circunscrever o ataque e identificar os alvos e os efeitos. Esses três parâmetros dependem tanto do conhecimento das intenções do adversário quanto das capacidades disponíveis. Da mesma forma que nos domínios físicos, o mapeamento do campo informacional é um pré-requisito para a detecção. Sua preparação antecipada a qualquer operação e seu enriquecimento permanente são decisivos.

O segundo desafio é a **análise dos ataques a fim de atribuição**, ou seja, a busca da origem dos ataques (país, empresa, grupo, indivíduo, etc.) até sua identificação formal e a sua designação pública pela autoridade – geralmente política (Boyer, 2020). No entanto, no contexto do ambiente informacional – onde os argumentos de marketing de proteção de dados podem às vezes questionar as medidas de segurança coletiva[24]– os métodos tradicionais de análise sistêmica são inoperantes. Considerada uma atividade de condução, a análise está, no entanto, fortemente ligada ao planejamento. Nesse sentido, planejar é decidir os pré-posicionamentos nas plataformas de informação para um melhor conhecimento do

[24] As plataformas de mensagens instantâneas como Whatsapp, Signal ou Telegram fazem da proteção dos dados pessoais um argumento de marketing, levando à uma falsa sensação de segurança e à criação de zonas cinzentas, limitando medidas de segurança coletiva dos Estados (escutas administrativas, antiterrorismo, etc.).

ambiente, preparar recursos (competências e pessoas) habitualmente muito distantes das atividades militares e, por fim, educar os responsáveis estratégicos sobre a necessidade da comunicação ao longo da cadeia de comando inteira, ou seja, até o mais alto nível políticos (MINARM, 2021).

Por fim, o terceiro desafio são **os mecanismos de resposta** aos ataques informacionais. Por natureza proteiforme, essa resposta se baseia nos dois desafios anteriores. Antes de tudo, ela visa proteger os públicos-alvo, em primeiro lugar as forças armadas e sua missão, mas pode também ser toda ou parte da opinião pública (Boyer, 2020). Essa proteção é necessariamente uma ação interagência. No entanto, ela deve incluir medidas ofensivas para retomar o controle do poder discursivo, manter a capacidade de inovar e retirar o sentimento de impunidade do atacante. De forma mais ampla, a superioridade informacional sugere a adoção de estratégias defensivas e ofensivas combinadas e sincronizadas, sob o risco de perder a iniciativa nesse campo de confrontação e de criar vulnerabilidades em outros domínios físicos.

Esses desafios mostram que a prontidão no campo informacional decorre só de uma postura permanentemente ativa, capaz de impor, ampliar e valorizar as mensagens em respeito do direto nacional e internacional (Marangé, 2021). A integração no processo de planejamento das dimensões de detecção, de atribuição e de resposta constituem um padrão mínimo de defesa.

3.2.4 O episódio de Gossi (Mali) contra a França

Em janeiro de 2013, as forças armadas do Mali enfrentam uma onda terrorista, decorrentes das aspirações independentistas históricas tuaregues e de grupos salafistas jihadistas. Conforme à Carta das Nações Unidas, a França responde ao pedido de assistência do Mali, iniciando a operação SERVAL, repelindo os terroristas no Norte, causando pesadas perdas. No entanto, progressivamente, os países do Sahel se envolvem em um longo combate assimétrico na região desértica de três milhões de km², ou seja, a metade da Amazônia, com geografia e demografia complexas. A situação levou a França a tornar seu dispositivo operacional mais amplo com um foco de longo prazo: a operação Barkhane (Lalanne, 2022).

Além disso, em maio de 2021, o golpe de Estado do Coronel Goita deu origem à fortes tensões políticas entre a França e o Mali. A junta militar no poder quer expulsar as forças de Barkhane, com o objetivo de alterar o alinhamento político-estratégico, ilustrada pela presença da empresa militar privada russa Wagner. Nesse contexto, em abril de 2022, surge o caso de Gossi, cidade maliana na região de Tombuctu. Esse caso ilustra um ataque informacional deliberado, visando desacreditar forças militares francesas em operação (Lalanne, 2022).

No processo da retirada francesa do Mali, o campo de Gossi é retrocedido às forças armadas malianas (FAMA) no dia 19 de abril de 2022. Enquanto suspeita-se da presença de membros do grupo Wagner desde o dia 20 de abril, o dispositivo de vigilância informacional francês detecta no mesmo dia na rede social Twitter uma publicação duvidosa. A conta suspeita, de um soldado aposentado, patriota maliano e analista político, acusa diretamente os soldados franceses de crimes de guerra. Imediatamente, forças francesas conduzem reconhecimentos aéreos na área. Pouco depois, os drones capturam imagens de um grupo de indivíduos enterrando cerca de cinquenta corpos sem vida, enquanto filmam a ação, a três quilômetros do campo (Roger, 2022).

O caso toma uma outra dimensão quando, no dia seguinte, a mesma conta publica conteúdos gráficos e atribui o massacre à França. Logo detectada, esta publicação desencadeou um processo militar de resposta informacional até o topo do Estado francês. A divulgação pública das imagens dos drones e o engajamento das esferas midiáticas de France24 e de Radio France Internationale (RFI) permitiram rapidamente fazer a luz sobre incoerências temporais. O dispositivo também permitiu demonstrar que a conta falsa, criada dois meses antes, usava uma foto de perfil utilizada na rede social russa VKONTAKTE, por uma pessoa originária da Colômbia. Enquanto a França criticou os métodos do grupo Wagner, o Mali apontou, para sua defesa, a ilegalidade do sobrevoo da zona pelos drones franceses - argumento infundado após a publicação do documento oficial o autorizando (Roger, 2022).

Exemplo de um ataque informacional no modelo de guerra híbrida, esse caso mostrou perfeitamente a contração do tempo e a continuidade do espaço físico e informacional no processo de seleção de alvos. Os mecanismos de resposta,

integrados desde o planejamento nos meios de execução, foram determinantes para um mapeamento preventivo do ambiente informacional e ações físicas para encontrar elementos de evidências. Além disso, a análise e a exploração em quase tempo real dos dados coletados foi uma etapa essencial, tanto pela remanência das informações na Internet quanto pelo engajamento do nível político e das mídias internacionais. A desinibição de certos Estados nas manobras informacionais ofensivas chama atenção das democracias cujo valores são os seus alvos (Lalanne, 2022).

4 CONEXÕES: AS CHAVES DO PRÓXIMO SALTO CONCEITUAL

Neste capítulo, faremos a aproximação entre os elementos teóricos da arte operacional, desenvolvidos no capítulo dois, e o conjunto das características do ciberespaço técnico e do campo informacional ilustradas no capítulo precedente. O objetivo será identificar, por meio de quatro noções-chave fundamentais do engajamento armado, conexões a fim de ter uma melhor compreensão das dinâmicas envolvidas nos conflitos modernos, bem como novas perspectivas a levar em consideração no planejamento militar. As quatro noções-chave são as seguintes: a iniciativa, a incerteza, a permanência e o comando.

4.1 As perspectivas do princípio da iniciativa

A doutrina da Organização do Tratado do Atlântico Norte (OTAN, AJP-3, 2019) define a iniciativa como o exercício da sua liberdade de ação, ou seja, com a capacidade de agir de maneira proativa, tomando decisões que moldam o curso das operações e influenciam o ambiente de combate antes das reações do inimigo. Nesse escopo, a ação no ciberespaço e no campo informacional aparece como um elemento-chave na busca por este princípio militar fundamental. Ela permite explorar novas dimensões de um conflito moderno por meio de três aspectos: a produção imediata de efeitos em profundidade; o alargamento do espectro da seleção dos alvos; e a facilitação da integração de posturas ofensivas e defensivas simultâneas com foco em objetivos positivos e negativos.

Em primeiro lugar, no contexto do ciberespaço e do campo informacional, a ação em profundidade procede da vontade do estrategista de contornar as defesas adversárias e afetar alvos críticos posicionados além da linha de frente geográfica. Ao contrário das ações militares convencionais, que frequentemente necessitam de tempo para mobilizar e desdobrar forças em profundidade, as operações cibernéticas e informacionais podem ser executadas instantaneamente e produzir efeitos imediatos. Essa capacidade de atacar profundamente e rapidamente dá às forças armadas uma flexibilidade estratégica e uma reatividade ampliadas. Oferecendo novas opções de respostas militares, aliada à versatilidade inerentes às operações híbridas, as capacidades cibernéticas e informacionais aparecem como particularmente poderosas para perturbar o adversário, antes de qualquer reação. Consequentemente, são ferramentas determinantes no ganho ou manutenção da iniciativa em favor da força.

Em segundo lugar, o ciberespaço e o campo informacional modificam radicalmente a situação na perspectiva da seleção de alvos. Ao ultrapassar o estrito quadro dos alvos físicos tradicionais, assim como as limitações geralmente impostas às forças armadas em desvantagem no fator operacional força, a seleção de alvos digitais e informacionais pode incluir diretamente pontos nevrálgicos do adversário, como infraestruturas críticas ou redes e sistemas de comando, controle, comunicações, computação, inteligência, vigilância e reconhecimento (C4IVR). Essa extensão do espectro dos alvos permite também uma total elasticidade na produção de efeitos, do mais elementar ao mais estratégico, sem mobilizar capacidades de destruição física. Ao integrar a seleção de alvos cibernética e informacional, combinada ou não com opções convencionais de fogos, as forças armadas podem enfraquecer o adversário de maneira mais sutil, mas igualmente mais efetiva. Ao perturbar as operações, semear a confusão e afetar o moral ou a credibilidade da estrutura política ou militar do adversário, a opção por uma linha de ação de largo espectro consistente permite não apenas uma tomada de iniciativa escalável conforme o nível de conflitualidade desejado, mas também alinhar as ações militares com objetivos estratégicos mais amplos. Assim, é uma ferramenta poderosa para fragilizar as relações entre os três pilares da trindade de Clausewitz do adversário.

Por último, a tomada de iniciativa só é possível quando as forças dispõem da liberdade de ação mínima. Essa visão destaca que a alternância das fases operacionais em que as forças adotam posturas ofensivas e defensivas se torna de importância maior. Mas, no ciberespaço e no campo informacional, essas fases são paralelas por natureza. Assim, pode-se produzir todo um espectro de efeitos ofensivos para degradar, perturbar ou neutralizar sistemas (no sentido tecnológico ou social) ou capacidades adversárias, ao mesmo tempo em que se implementam mecanismos de proteção e se lançam operações de defesa. Simultaneamente, essa flexibilidade também se exerce na busca por objetivos tanto positivos – quando se quer mudar uma situação ou conquistar uma vantagem – quanto negativos – quando se quer preservar o *status quo* ou manter uma conquista. Essa liberdade oferece múltiplas opções ao estrategista. Por consequência, a iniciativa é favorecida tanto pela capacidade de ajustar o nível de fricção conforme o nível de conflitualidade desejado, quanto pelo aumento da incerteza para o adversário. Ao buscar sistematicamente esse fator de superioridade operacional, o estrategista impõe ao adversário um confinamento em uma postura reativa, ao mesmo tempo em que a força persegue a consolidação de suas próprias defesas.

Em um conflito híbrido com dimensões cibernéticas e informacionais, essa conexão entre a profundidade e o caráter imediato da ação dá à iniciativa uma dimensão radical e ilustra perfeitamente a necessidade de uma abordagem complementar na arte operacional, fazendo do campo informacional e do ciberespaço uma linha decisiva da manobra, em qualquer nível de comando. Uma etapa de análise detalhada da manutenção da iniciativa surge como uma necessidade e uma perspectiva de evolução do planejamento das operações.

4.2 As perspectivas do princípio da incerteza

Como vimos anteriormente, o ciberespaço e o campo informacional trazem novas opções para manter a iniciativa. Eles também desempenham um papel fundamental na busca constante de um objetivo maior: reduzir a incerteza, seja ela originada de lacunas da inteligência, e mitigar a influência exercida pelo adversário, inclusive nas zonas cinzentas (Boyer, 2020). Para isso, o alinhamento no quadro operacional é essencial: apenas uma ambição estabelecida no mais alto nível do

Estado e uma orientação coerente dos sensores de inteligência permitem que os órgãos encarregados da antecipação conduzam uma prospecção, uma antecipação estratégica e um planejamento pertinentes. Minimizar a sombra que pesa sobre a tomada de decisão passa, no entanto, pelas três novas conexões seguintes.

A primeira conexão a destacar é aquela que existe entre a superioridade informacional proporcionada pelos armamentos de nova geração e o controle completo e permanente dos riscos cibernéticos associados. De fato, buscando um objetivo operacional legítimo, essa superioridade repousa quase exclusivamente em sistemas com arquiteturas digitais, às vezes conectadas e frequentemente associadas a tecnologias de uso comum (softwares Microsoft, máquina virtual Java, etc.). Nesse contexto, reduzir a incerteza é, antes de tudo, uma tomada de consciência de nossa própria vulnerabilidade: o funcionamento da maioria das redes de C4IVR e das capacidades operacionais está sujeito a falhas que podem surgir a qualquer momento, por meio de softwares abertos na Internet, nas mãos de especialistas que as vendem ao maior lance, ou nos laboratórios de serviços de inteligência estatais. A incerteza só pode ser dissipada com um domínio perfeito das tecnologias e a implementação de uma postura permanente de ciberdefesa robusta e escalável, que se apoia em uma inteligência de interesse cibernético, medidas proativas e protocolos de resiliência testados em exercícios regulares de ciberataques – simulados ou reais. Assim, no conflito tecnológico, a primeira das incertezas é também a primeira das surpresas, quando um míssil não sai de seu silo no momento desejado, ou quando uma mensagem não é transmitida, como os ucranianos isolados durante o ataque contra a constelação de satélites *Viasat* no dia antes da invasão russa.

A segunda conexão é uma questão de segurança operacional: a controvérsia da presença de dispositivos conectados no bolso dos soldados em operações. Levando em consideração as características do campo informacional e da camada técnica do ciberespaço, vale ressaltar que esses dispositivos representam uma nova superfície de ataque contra a força. O controle de seu uso é geralmente muito baixo e muitas vezes se baseia apenas em medidas organizacionais e na disciplina individual, em um contexto onde o smartphone pode às vezes representar, na linha de frente, o último elo com o círculo social e familiar. Essa conexão permanente é,

portanto, principalmente a origem de uma nova fonte de incerteza para o estrategista. Por outro lado, um potencial ponto de fragilidade para a força, também o é para o adversário. Assim, a apropriação de uma cultura de cibersegurança pelos soldados, ou seja, o uso de dispositivos seguros e o respeito a protocolos rigorosos em relação aos seus dispositivos pessoais, têm uma contrapartida: a exploração sem reservas da conexão dos soldados adversários, cujas falhas representam uma oportunidade para dissipar a névoa da guerra que envolve o inimigo. Novamente, o planejamento deve inclinar essa relação de forças para o lado favorável, especialmente porque o efeito induzido no moral pode ser particularmente poderoso.

A terceira conexão é herdada de uma das características do jogo de *go* destacada anteriormente, segundo a qual o valor de uma pedra não está ligado apenas às suas qualidades intrínsecas, como no xadrez (alcance, velocidade, flexibilidade de uso, etc.). Essa conexão liga a ideia contraintuitiva de se implantar voluntariamente nas zonas cinzentas e o dilema do estrategista entre a intenção firme de empregar a força e o controle da escalada do conflito. Na perspectiva do *go*, o valor de uma peça é aquele que o estrategista lhe atribui no momento em que ele a coloca nas linhas do tabuleiro. Assim, é o estrategista quem atribui um valor operacional às tropas, tanto quanto as tropas colocam sua capacidade à disposição do estrategista. No ciberespaço e no campo informacional, essa perspectiva torna possível o pré-posicionamento de capacidades em zonas onde a névoa da guerra é tão espessa para os dois estrategistas face a face. O estrategista não tenta mais dissipar a incerteza para tomar uma decisão, mas toma a decisão de investir na área da incerteza e, até certo ponto, de densificá-la para o adversário. A névoa da guerra então oculta toda a preparação, a condução e, às vezes, parte ou todos os efeitos produzidos aos olhos da força inimiga. As manobras nas e a partir das zonas cinzentas, como as camadas não referenciadas da Internet (*Deepweb, Darkweb*) ou nas plataformas abertas usadas diariamente por centenas de milhões de usuários, tornam-se quase invisíveis até o momento em que os impactos concretos são difíceis de contrariar. A complexidade de imputar e atribuir ataques nesse meio e nesse campo de confrontação também concede ao estrategista uma maior variedade de opções e, acima de tudo, eleva potencialmente o limiar da escalada do

conflito, mantendo-o em um nível aceitável, resolvendo em parte o dilema do estrategista ao usar a incerteza como cobertura.

Em um conflito híbrido, a incerteza não se aplica apenas a um lado dos beligerantes. O ciberespaço e o campo informacional são áreas capazes de a reduzir, inclusive nos meios físicos. A superioridade informacional, pelo domínio tecnológico e pela preparação humana e organizacional, surge como um novo fator crítico em um conflito. No entanto, a incerteza é também uma oportunidade de atuar em um espectro amplo, em profundidade, de maneira anônima, à velocidade da luz e nos níveis dos mais baixos aos mais altos, inclusive político. No planejamento das operações, o uso ou a ampliação da incerteza representa uma alavanca poderosa a incluir na reflexão. Em qualquer linha de ação, ela favorece a criação de efeitos de impotência na reação do inimigo, a criação de fatos consumados e a manutenção da iniciativa.

4.3 As perspectivas do princípio da permanência

A incerteza e a iniciativa formam um primeiro eixo de melhoria no exercício da arte operacional no planejamento das operações. No entanto, nesta associação, o tempo surge como uma dimensão indispensável à luz das características intrínsecas do meio e do campo examinados no capítulo três. Assim, a ação no ciberespaço e no campo informacional exige a adoção de uma postura permanente específica, em todas as etapas da antecipação e da execução das operações. Essa permanência se manifesta por meio de três novas conexões.

A primeira conexão, ligada à noção de permanência, implementa o novo paradigma de conflitualidade e o uso do ciberespaço e do campo informacional para ataques abaixo do limiar do conflito. Marcado pelo retorno à competição entre grandes potências, o mundo globalizado também experimentou um encolhimento do tempo e do espaço graças às tecnologias da informação. As consequências são diretas: as instituições são obrigadas a manter uma vigilância ampla e constante, bem como desenvolver capacidades de monitoramento e resposta que funcionem de forma contínua. Nesse contexto, a detecção de ameaças e as contramedidas antes da ocorrência de danos significativos tornaram-se premissas para as forças armadas, cujo engajamento no terreno é sempre suscetível a manipulações que

podem gerar riscos de descredibilização. Escaladas atuais para o confronto aberto na Ucrânia e na Faixa de Gaza mostram, no entanto, que se o modelo de conflitualidade permanece gradual – na medida em que existe uma progressividade entre competição, contestação, confrontação –, as ações nos ambientes e campos imateriais podem ser de alta intensidade desde o tempo da competição (como no caso de Gossi).

A segunda conexão que caracteriza o critério de permanência é aquela entre a aquisição de novos conhecimentos e a ampliação da abordagem global das operações sob o prisma da interagência. Assim, a criação de novas parcerias, militares ou não, nacionais e internacionais, é um fator-chave para fortalecer a resiliência frente aos ataques cibernéticos e informacionais. Como demonstrou a reação dos exércitos franceses no caso de Gossi, a diversificação das expertises – operacionais, técnicas ou psicológicas – e dos recursos – de captação, de influência e de difusão – é indispensável para enfrentar os novos desafios desta natureza. A coordenação com esses novos parceiros é uma competência nova para a instituição militar. Por um lado, ela impõe uma convergência de esforços para impor uma narrativa compartilhada, global e robusta. Por outro lado, a instituição precisa ser mais flexível quanto à confidencialidade das informações, da mesma forma que a operação Barkhane disponibilizou imagens classificadas de um drone ao canal de televisão internacional.

Por fim, a terceira conexão que ilustra o princípio de permanência é aquela entre a proteção da população e do modelo democrático, e a consideração das intenções adversas em todo o ciclo de antecipação. Nesse caso, é importante colocar em perspectiva a salvaguarda dos fundamentos do Estado com a ajuda da prospectiva, da antecipação estratégica, do planejamento e da condução das operações. Além disso, nossas sociedades democráticas tornaram-se alvos permanentes para uma grande diversidade de grupos mal-intencionados cujos objetivos a curto, médio e longo prazo são múltiplos: políticos, econômicos ou ideológicos. Em corolário, a vigilância e a informação da população poderiam, ao longo do tempo, tornar-se uma tarefa básica de poder, cuja dimensão de defesa é indissociável das forças armadas e da adoção de mecanismos proativos de antecipação. As ameaças emergentes e as agressões repetidas no ciberespaço e no

espaço informacional tornam ainda mais exigente a avaliação da situação do campo de batalha móvel e imaterial. No final, ao impor um ritmo superior às operações, a permanência consolida, no entanto, as abordagens "paralela" e "sequencial" do processo de planejamento das operações.

O planejamento da resposta às ações no ciberespaço só pode ser eficaz ao enfrentar o desafio da permanência. Em um paradigma de conflitualidade fluido e incerto, a antecipação e a convergência buscada na colaboração interagências são preocupações-chave para o estrategista. Fator de atrição por natureza, tanto para os materiais, quanto para os seres-humanos, o tempo surge no planejamento das operações híbridas como um parâmetro maleável. Assim, o tempo útil para o estrategista se tornou a permanência.

4.4 As perspectivas do princípio do comando

Após a incerteza, a iniciativa e a permanência, há um ponto essencial a ser abordado na mudança da abordagem do planejamento de operações para enfrentar os desafios das camadas do ciberespaço. Assim, o comando integra essas três noções iniciais em um quadro abrangente. Ele ilustra a nova realidade das operações com uma visão mais profunda, um salto conceitual comparável ao de Svechin ao conceber a arte operacional. Novamente, três reflexões destacam as perspectivas do comando.

A primeira reflexão decorre das características intrínsecas do ciberespaço. Ela conecta, por um lado, a intensidade dos efeitos produzidos no ou a partir do ciberespaço e, por outro, a rapidez com que são provocados. Essa fulminância, considerada como um princípio da guerra segundo o Almirante Labouérie (1933-2016), impõe uma organização da cadeia de comando com maior verticalidade e fluidez. Considerando os parágrafos anteriores, a contribuição de uma boa circulação do fluxo de informações e de inteligência entre os níveis de comando é fundamental. Recebendo continuamente uma matéria-prima mais confiável, permitindo sistematicamente surpreender o adversário e afinar a percepção, o comando assegura tomadas de decisão mais resilientes e proativas diante da incerteza. Colocando alavancas de decisão e ação adequadas em cada nível de comando abaixo, o estrategista antecipa e reduz a eficácia dos golpes recebidos,

não pela rapidez e intensidade com que eles são desferidos, mas pela clareza com que eles são percebidos. Sempre existe um curto intervalo de tempo para que o comando possa transformar um ataque cibernético ou informacional significativo em um fracasso salvador, ou seja, uma agressão abaixo do limiar potencialmente devastador em um fiasco retumbante.

A segunda reflexão aborda um dos três pares fundamentais da arte operacional, que trata da alternância temporal entre operações ofensivas e defensivas. No terreno físico das operações, essa alternância é exclusiva, ou seja, as tropas estão em uma fase ofensiva ou defensiva, mas não em ambas ao mesmo tempo. No entanto, o caráter imaterial do ciberespaço modifica profundamente esse modelo. Assim, em todas as camadas do ciberespaço, as duas linhas de ação são adotadas simultaneamente. Dada a diferença nas habilidades, métodos e ferramentas empregadas, essa dualidade exige do comando uma agilidade constante, a criação de unidades especializadas ofensivas e defensivas distintas e uma avaliação situacional abrangente. A abordagem temporal da arte operacional de Svechin é fragilizada pelo princípio da alternância. Nas camadas técnicas do ciberespaço, os recursos são suficientemente diferenciados entre ataque e defesa, tornando imperativa a criação de unidades especializadas eficaz na distribuição de missões e na prevenção de interferências. Em contrapartida, no campo informacional, o impacto não é neutro. Assim, os recursos (plataformas, avatares, etc.) revelados[25] durante uma operação geralmente se tornam indisponíveis para uma outra, ou podem representar um perigo para outros recursos ainda adormecidos. Para o comando, o consumo de recursos cibernéticos, especialmente os ofensivos, pode frequentemente se revelar um dilema significativo.

A terceira e última reflexão decorre da dialética entre a instabilidade do campo de batalha no ciberespaço e no espaço informacional e a necessidade de fixar uma avaliação da situação no processo de planejamento para decidir uma linha de ação e limitar os recursos a serem mobilizados. Assim, ao contrário de um espaço físico onde a geografia é estável, a cartografia do ciberespaço e do espaço informacional

[25] Um dispositivo de ciberinfluência usado para uma operação ofensiva ou defensiva, é geralmente considerado como consumido, ou seja, é identificado como um vetor artificial estatal. A reciclagem é perigosa. Por exemplo, uma conta de rede social usada para desmantelar um grupo terrorista não funcionará em um outro grupo.

evolui continuamente, tornando o campo de batalha dinâmico e imprevisível. Além disso, essa cartografia não é simétrica, pois a percepção dos dois beligerantes é, por natureza, distinta, e o conhecimento absoluto desses ambientes é inalcançável. Essa reflexão remete às expressões de necessidades em materiais e dados geográficos, a terceira etapa das quatro fases de planejamento segundo Svechin abordadas no capítulo dois. O conflito moderno, portanto, apresenta novos desafios para o estrategista: o custo elevado do desenvolvimento de armas digitais (técnicas ou informacionais) em um contexto instável que pode torná-las inoperantes da noite para o dia, a reavaliação contínua da cartografia digital em frente da organização muito rígida dos estados-maiores e, no final, o caráter multidimensional do teatro de operações, que torna ilusório qualquer esforço para modelar uma situação única em múltiplos domínios.

No planejamento das operações, a estrutura de comando muda pouco a pouco para uma visão mais integrada que considera os fatores de liberdade de ação (estratégica, operacional e tática), a criação de incerteza e a distorção do tempo pelo adversário. Embora a essência da arte operacional permaneça a mesma, essa abordagem permite uma agilidade maior para alternar entre diferentes linhas de ação, maximizando a exploração dos resultados dos combates como matéria-prima para a vitória.

5 CONCLUSÃO

Este trabalho se propôs a responder aos desafios da integração das características do ciberespaço e do campo informacional nos processos de planejamento militar. Para isso, a pesquisa apresentou consecutivamente dados teóricos, analisou casos práticos ilustrativos e destacou conexões-chave para um novo salto conceitual que exige uma abordagem multidomínio.

No segundo capítulo, exploramos os princípios fundamentais da arte operacional. Por meio de referências de reflexões estratégicas e da abordagem lúdica de jogos de tabuleiro, elaboramos um retrato da disciplina conforme o pensamento do General soviético Alexander Svechin. A conceitualização da arte operativa aparece como um salto conceitual importante na percepção do espaço, do tempo e da visão conjunta das operações, assim como um jogador de xadrez

descobrindo o jogo de *go*. Na perspectiva do planejamento e da condução da guerra, o nível intermediário de comando entre a estratégia e a tática revolucionou a visão do estrategista e a tomada de decisão. O pensamento de Svechin transcendeu o de Clausewitz em uma perspectiva soviética, tornando os resultados dos combates como uma matéria-prima e ressaltando a visão global de um conflito. No século XXI, impulsionado pelas tecnologias da informação, o comando operacional se arma de ambições políticas fortes, de novas técnicas de inteligência e de um novo paradigma de conflitualidade. Este nível de comando, criado para vencer nas guerras complexas, não aparece, portanto, apenas como uma ferramenta para continuar a política por outros meios, mas como uma engrenagem essencial, ou seja, como uma mão na qual os políticos entrega a sobrevivência da Nação e das instituições. Os jovens oficiais superiores têm, portanto, um dever imenso sobre seus ombros, o de pensar a arte operacional moderna e preparar aquela do futuro.

No terceiro capítulo, definimos e exploramos as várias camadas do ciberespaço. Assim, as camadas técnicas e semânticas delineiam um novo meio, o ciberespaço físico, e um novo campo de confrontação, o campo informacional. As características foram ilustradas por meio de situações operacionais recentes e concretas. O ciberespaço e o campo informacional são espaços comuns onde se exercem novas vontades de poder. Alguns Estados exploram falhas técnicas e cognitivas para impor suas narrativas e alcançar a credibilidade dos modelos democráticos. Fortemente expostas, as sociedades gradualmente medem a ruptura que ocorre na percepção da intensidade da guerra, que agora é travada no espaço digital e, muitas vezes, abaixo do limiar do conflito armado. As tecnologias da informação trazem novas dimensões ao campo de batalha e, portanto, novas variáveis à arte operacional, onde a cartografia, o alerta e a resposta são prismas que evoluem de maneira contínua.

No quarto capítulo, identificamos quatro noções-chave que representam critérios decisivos a serem considerados para alcançar o próximo salto conceitual no planejamento das operações e explorar aspectos ainda pouco abordados da arte operacional. Essas noções-chave foram definidas em múltiplos pares de conceitos discutidos ao longo da pesquisa. Levando em conta os desafios do ciberespaço, a evolução da arte operativa parece passar por uma revisão da percepção do tempo

útil para o estrategista (a permanência), a utilização da incerteza, o domínio da iniciativa e a adoção de novas práticas de comando. Essas novas perspectivas poderiam romper as barreiras entre o planejamento e a condução conjunta das operações, tornando a arte operacional moderna um nível de comando permanente e central. Á origem pensada como um nível de comando intermediário, ou seja, uma disciplina dobradiça, a arte operacional represente em realidade a pedra angular do espírito e da prática militar.

A principal importância deste trabalho de pesquisa não reside apenas na descoberta dos pensadores importantes da estratégia militar ao longo da história, mas também na reflexão sobre como conectar essas ideias com os desafios atuais. Esta pesquisa não se limitou a uma simples análise dos princípios estabelecidos no passado. Ele permitiu sobretudo entender que a revolução digital esta apenas começando. Como um símbolo, Clausewitz escreveu, no seu livro I *Da Guerra*, que os gênios seriam mais aqueles que examinam do que aqueles que criam. Desde então, tornou-se claro para os estrategistas militares que defender suas convicções é válido apenas se elas forem fruto do rigor e da experiência de um espírito analítico. A expansão dos limites do campo de batalha, o ciberespaço e o campo informacional mudaram as regras do jogo. Atualmente, a criatividade, a inteligência emocional e o gosto pela abordagem técnica norteiam mais do que nunca para as altas esferas do comando. O mais surpreendente é que essas caraterísticas, antigamente vistas como desfavoráveis na arte de comandar, estão alinhadas com qualidades fundamentais dos líderes de guerra: energia, firmeza, constância e caráter.

REFERÊNCIAS

BAECHLER, Jean. Artigo **« Guerre et Paix »**, in Dictionnaire de la pensée sociologique, Collectif. Ed. Presses Universitaires Françaises. 2005.

BIHAN, Benoist. LOPEZ, Jean. **Conduire la guerre – Entretien sur l'art opératif**. Ed. Perrin. 2023.

BOYER, Bertrand. **Guérilla 2.0, guerre irrégulières dans le cyberespace**. Ed. Les éditions de l'école de guerre. 2020.

BURKHARD, Thierry. **Vision stratégique du Chef d'état-major des armées (CEMA).** 2021.

DABILA, Anthony. **L'engagement militaire, une étude de sociologie comparée**. Tese Universidade Paris Sorbonne, 2013.

LALANNE, Charlotte. L'Express. **"Vrai-faux charnier" au Mali : entre Paris et Moscou, la guerre de l'information se durcit.** 23/04/2022. Artigo.

JORNAL OFICIAL DA REPUBLICA FRANCESA (JORF) 0219. Comissão de enriquecimento da língua francesa, Vocabulário da defesa: ciberdefesa. 19/09/2017.

LIDDEL HART, Basil H. **Stratégie**. Ed. Perrin. 1999.

MARANGÉ, Céline e QUESSARD, Maud. **Les guerres de l'information à l'ère numérique.** Ed. Presses Universitaires de France. 2021.

McLUHAN, Marshall, **Os Meios de Comunicação Como Extensões do Homem.** Ed. Cultrix.1964.

MILLEQUANT, Benoit. **Jeu de go et géopolitique de la Chine : intérêts et limites d'une lectura "ludiques" des conflits.** Revista Conflits. 2021. Artigo.

MINARM (Ministère des Armées). **Elementos públicos de doutrina militar de luta informática de influencia (L2I).** EMA/COMCYBER. 2020.

MINARM (Ministère des Armées). **La prospective opérationnelle. Pourquoi ? Comment ?** DC-007_PO. 2022.

MINARM (Ministère des Armées). **Política ministerial de luta informática defensiva**. 2019.

MINISTÉRIO DA DEFESA. **MD31-M-07: Doutrina Militar de Defesa Cibernética.** 2023.

OLSEN, John Andreas. VAN CREVELD, Martin. **The Evolution of Operational Art - From Napoleon to the Present.** Ed. Oxford University Press. 2010.

PENISSON, Bernard. **Histoire de la pensé stratégique, De Sun Zi au nucléaire.** Ed. Ellipses poche. 2019.

RID, Thomas. **Cyberwar will not take place.** Ed. Oxford University press. 2013.

ROGER, Benjamin. Jeune Afrique. **Mali, à Gossi, la France accuse Wagner « d'attaque informationnelle ».** 22/04/2022. Artigo

SAUCIN, Joel. **Le jeu de go, modèle analogique pour les sciences humaines**. Ed. Les certitudes de l'Aurore. 2004.

SCHAFER, Valérie. **L'information mondialisée et individualisée.** EHNE (Encyclopédie d'histoire numérique de l'Europe. 23/06/2020. Artigo

Secretaria Geral da Defesa e da Segurança Nacional (SGDSN). **Guia para a elaboração de uma política de segurança de sistema de informação (PSSI).** 2004.

VON CLAUSEWITZ, Carl. **De la guerre - Livre 1.** Ed. GF Flammarion. 2014.

Revue Nationale Stratégique (RNS). Presidência da República francesa. 2022.

Ciberoperações russas contra a Ucrânia: Declaração do alto representante (Josep Borrell) em nome da União Europeia. Artigo do dia 10 de maio 2022. https://www.consilium.europa.eu/pt/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/. Concelho Europeu / Concelho da União Europeia. 2021.

RESIST 2 Counter-disinformation toolkit. UK Government Communication Service. 2022. https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/