ISSN: 2525-457X
Análise Estratégica
v. 30, n.3, jun./ago. 2023

MAPEAMENTO PRELIMINAR DA TRAJETÓRIA DAS DISCUSSÕES SOBRE "AMBIENTE INFORMACIONAL" E "GUERREAR INFORMACIONAL"

"INFORMATION ENVIRONMENT" AND "INFORMATION ENVIRONMENT": A PRELIMINARY MAPPING OF CONCEPTS

EUGENIO DINIZ

RESUMO

Visa-se aqui a um esforço inicial de mapeamento da trajetória das ideias de "guerra informacional" e/ou "guerrear informacional", "ambiente informacional" e "zona cinzenta", conforme a literatura e publicações doutrinárias, principalmente do Exército dos Estados Unidos da América. Trata-se de um esforço preliminar, cujo propósito é permitir, num momento posterior, uma avaliação mais rigorosa de tais ideias. Ainda assim, algumas dificuldades já são examinadas. Embora documentos doutrinários e a literatura que os embasa direta ou indiretamente apresentem sugestões interessantes para reflexão e aprofundamento, nem tudo é consistente com vertentes mais sofisticadas da discussão, enquanto outras parecem ter o potencial de conflitar fortemente com valores democráticos. Além disso, ideias como a da "zona cinzenta" parecem pôr em xeque a própria ordem internacional baseada em regras que se pretende proteger. Por fim, várias delas parecem conceitualmente frágeis e inconsistentes, demandando mais reflexão.

Palavras-chave: Ambiente Informacional; Guerrear Informacional; Zona Cinzenta; Operações Informacionais.

ABSTRACT

A preliminary effort of tracking the trajectory of the ideas of "informational war" and/or "informational warfare", "informational environment" and "gray zone", according to the literature and doctrinal publications, mainly from the US Army, is what is undertaken here. The purpose is to enable a more rigorous assessment of such ideas at a later moment. Nevertheless, some problems are already addressed here. While doctrinal documents and the literature that directly or indirectly underpins them might present some insight and food for thought, not all of them seem consistent with more sophisticated strands of the discussion, while others appear to conflict with democratic values. Moreover, ideas such as "the gray zone" seem to call into question the very rules-based international order they are intended to protect, and some others seem conceptually flawed and inconsistent.

Keywords: Information Environment; Information Warfare; Gray Zone; Information Operations.

O AUTOR

Professor do Departamento de Relações Internacionais da Pontifícia Universidade Católica (PUC-MG). Diretor Executivo e fundador da Synopsis - Inteligência, Estratégia, Diplomacia. É membro do International Institute for Strategic Studies - IISS (Londres) e da International Association for Security and Intelligence Studies - INASIS. É pesquisador 1C do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq). Pesquisador contratado do Núcleo de Estudos Prospectivos do Centro de Estudos Estratégicos do Exército (NEP-CEEEx) no ciclo 2023-2024.

1 INTRODUÇÃO

> *"Em seu sentido estrito, guerra é combate; pois o combate é o único princípio eficaz na atividade tão variada que, num sentido mais abrangente, se chama guerra. Mas a guerra é uma prova das forças morais e físicas por meio destas últimas."*
> "*Ambas* [a prostração das forças do inimigo e a ocupação de seu território] *podem ter sido alcançadas, e, ainda assim, a guerra, isto é, a tensão hostil e a ação das forças hostis, podem não ser tidas como concluídas, desde que a* vontade *do inimigo não tenha sido conquistada, ou seja, sem que seu governo e seus aliados tenham decidido assinar a paz ou que o povo esteja disposto a submeter-se.*"
> "*Com o termo 'informação' queremos designar todo o conhecimento que um homem tem sobre seu inimigo e sobre seu país e, por conseguinte, os fundamentos de suas ideias e empreendimentos.*"
>
> (Carl von Clausewitz, *Da Guerra*)[1]

Não é de hoje que se sabe que levar o oponente (suas forças, suas lideranças, sua população) a não querer lutar mais é um aspecto crucial da guerra; que, nela, a principal maneira pela qual influenciar sua vontade é pela ação das forças combatentes; e que interferir na sua capacidade de obter e transmitir informações úteis e válidas pode comprometer sua atividade, sua avaliação da situação e sua disposição para continuar ou não lutando, idealmente levando-o a aceitar, com o mínimo de custos de nossa parte, um resultado que nos seja mais favorável. Como essa interferência pode ocorrer depende das possibilidades disponíveis para cada sociedade em cada momento histórico específico.

Por exemplo, se as informações têm que ser obtidas por observação visual (com ou sem o auxílio de algum dispositivo óptico simples, como luneta ou binóculo, ou, posteriormente, até mesmo câmeras fotográficas), medidas de defesa passiva como camuflagem, ocultamento, dispersão, chamarizes podem ser suficientes para induzir o oponente a erros de avaliação. Se o oponente depende de espiões ou informantes, é possível identificar e vigiar ou eliminá-los; ou levá-los a fornecer informações falsas, consciente ou inconscientemente; ou, ainda, plantar falsos informantes ou agentes duplos. Se as informações e mensagens têm que ser transmitidas por um mensageiro a pé ou a cavalo, é possível interceptá-lo e, eventualmente, substituí-lo; ou, sub-repticiamente, substituir a mensagem original por uma falsa. As telecomunicações com fio (telégrafo e, depois, telefone) ofereceram novas e óbvias possibilidades de interceptação e interrupção das comunicações, mas ainda sem grandes exigências técnicas e organizacionais. Por sua vez, a única forma de comunicação em maior escala então existente, os jornais, era caracterizada por veículos eminentemente locais e regionais, com circulação restrita, fazendo com que não compensasse empregar grandes esforços junto à população – que, de resto, não era amplamente alfabetizada.

Já o uso do espectro eletromagnético para obtenção de informações (p. ex., radar, infravermelho) e sua transmissão (p. ex., rádio, televisão); a proliferação do registro de imagens (fotografias, filmes, vídeos); novas plataformas para sensores e transmissores (aeronaves, satélites); o surgimento das grandes empresas jornalísticas, da indústria cinematográfica e da televisão; a alfabetização generalizada; e o consumo de massa multiplicaram as oportunidades para a produção e

[1] Tradução livre, adaptada da de Teresa Barros Pinto Barroso, em Clausewitz (1979), cotejada com o texto alemão (CLAUSEWITZ, 1999 [1832]) e com a tradução de Michael Howard e Peter Paret (CLAUSEWITZ, 1989). Por razões que não podem ser exploradas aqui, nenhuma tradução que eu conheço do *Da Guerra* pode ser considerada plenamente satisfatória.

a circulação de informações. Por outro lado, também ampliaram as possibilidades de interceptação, despistamento e, como novidade de maior vulto, de levar informações (verdadeiras ou falsas) diretamente à população do oponente, sem intermediação de governos, furando bloqueios impostos por censores. Era possível, ainda, convencer ou aliciar repórteres ou editores nas grandes empresas jornalísticas, ou até mesmo "plantar" jornalistas com o objetivo de divulgar informações de interesse próprio. Atuar nesse contexto, porém, exigia significativa especialização técnica e investimento de recursos organizacionais, resultando no aumento da complexidade organizacional de forças armadas no mundo todo. Para além das mudanças conspícuas (surgimento da aviação, das forças aéreas e de suas componentes espaciais; da arma de Comunicações e especializações semelhantes nas diversas forças), houve a proliferação de atividades e termos, com suas especializações organizacionais, que marcaram a vigência desse ambiente com tais características: "guerrear psicológico" e "operações psicológicas"; medidas, contramedidas e contracontramedidas eletrônicas ou "guerrear eletrônico"; comunicação social, comunicações estratégicas, propaganda, etc.

Porém, a partir dos anos 1990, vários processos então em curso consolidaram-se e vêm convergindo:

a. inicialmente, o surgimento dos canais de televisão dedicados exclusivamente a notícias impôs uma nova dinâmica em sua produção, com aumento dos incentivos para a produção de "furos" jornalísticos e consequente diminuição relativa dos incentivos para checagem e confirmação de informações e produção de análises aprofundadas das notícias;

b. a ampla difusão do uso dos microcomputadores, tanto para uso pessoal, quanto profissional, comercial e governamental, aumentou exponencialmente a capacidade socialmente disponível de armazenamento e processamento de informações;

c. o surgimento e a expansão da Internet, levando também a um aumento exponencial das transações por via eletrônica e a distância, tornando praticamente desprezíveis os custos da transmissão de mensagens e informações, permitindo a praticamente todos os indivíduos com acesso a ela comunicar suas ideias e impressões por meio de páginas, sítios, blogs, etc., e, num segundo momento, canais de vídeo e mídias sociais de ampla repercussão;

d. ainda como consequência da expansão da Internet, vários setores de atividades vêm sendo redefinidos e transformados, com destaque para o comércio *online,* o setor financeiro, o jornalismo e a publicidade;

e. a possibilidade de comunicação em redes privadas, fora da Internet, transformou as comunicações internas das organizações e o acesso a seus dados;

f. a digitalização de imagens e de sons facilitou e barateou a sua produção, armazenamento e circulação;

g. a proliferação de sensores embutidos em múltiplos equipamentos (desde scanners em caixas registradoras a sensores de distância utilizados em carros) e de plataformas para sensores (com destaque para satélites e drones) contribuiu significativamente para a multiplicação da disponibilidade de dados para serem armazenados, processados, analisados;

h. a expansão das redes de computadores fez surgir o fenômeno do ciberespaço como espaço de trocas e transações, e potencializou a capacidade de processamento de informações graças ao amplo acesso a bancos de dados, que, por sua vez, puderam tornar-se muito extensos, exatamente em função da facilidade de obtenção (principalmente pela multiplicação de sensores diretamente

associados a equipamentos), armazenamento, processamento e acesso e transmissão de dados;

i. a partir de várias dessas transformações, surgiram as diversas mídias sociais, ampliando os canais de interação entre pessoas no mundo inteiro;

j. o surgimento da telefonia celular; a partir da terceira geração de serviços móveis (3G), o acesso a redes de computador pela infraestrutura de prestação de serviços de telefonia móvel, e o surgimento dos diversos modelos de *smartphones* intensificaram os processos acima;

k. as capacidades de processamento e análise de dados para categorização e recomendação foram dramaticamente aumentadas a partir de diversas técnicas de inteligência artificial; e

l. como consequência de todos os processos acima, os processos de produção e circulação de informações foram dramaticamente alterados, com particular impacto para a propaganda, a publicidade, o jornalismo, a indústria de bens audiovisuais, afetando significativamente o modo como a circulação e o debate de ideias ocorrem na sociedade – mas afetando também inúmeras outras indústrias.

Desde então, novos termos começaram a circular com mais intensidade, como "ciberguerra" ou "guerra cibernética" e suas "operações cibernéticas"; "guerra informacional"[2] ou, num sentido mais restrito, "guerra de informações", com suas "operações de informação" ou "operações de influência". Outros tiveram uma vida mais curta, ou, pelo menos, tornaram-se menos corriqueiras a partir de um certo momento, como "*netwar*" ou, ainda, "guerrear informacional estratégico" (MOLANDER et al., 1996). Em alguns casos, algumas das atividades já existentes anteriormente passaram a ser vistas à luz dessas novas propostas de entendimento, como "comunicações estratégicas" ou "operações psicológicas" (rebatizadas, no caso dos EUA, como "operações militares de apoio informacional" ou MISO). Entretanto, com o início das hostilidades na Ucrânia, em 2014, e o rápido sucesso da anexação da Crimeia pela Rússia, houve novo impulso à discussão, trazido pela ideia de "guerra híbrida" que se associou à ação russa, levando a uma ampla discussão sobre o que seria a "guerra informacional" no novo "ambiente informacional". Assim, introduziram-se novas ideias que, mais recentemente, passaram a fazer parte das publicações doutrinárias oficiais dos EUA e da Organização do Tratado do Atlântico Norte (OTAN) – como a ideia de "zona cinzenta" – e, no mínimo, reenquadrando outras noções – como, por exemplo, a de "guerra cibernética".

Visa-se aqui a um esforço inicial de mapeamento da trajetória das ideias de "guerra informacional" e/ou "guerrear informacional", "ambiente informacional" e "zona cinzenta" que foram formalizadas doutrinariamente, como referido. Trata-se de um esforço preliminar, cujo propósito é permitir, num momento posterior, uma avaliação mais rigorosa de tais ideias. Como se trata de um estudo feito no âmbito do Núcleo de Estudos Prospectivos do Centro de Estudos Estratégicos do Exército, privilegiar-se-ão, quando for o caso, textos e publicações que lhe possam ser mais afeitos.

Inicialmente, porém, é importante fazer algumas ressalvas. Em primeiro lugar, o emprego dos termos não é consistente ao longo dos textos estudados. Fique entendido, então, que o significado de um termo utilizado em qualquer momento deste ensaio refere-se, em princípio, ao empregado pelo texto que estiver sendo examinado mais detidamente naquele ponto; se, em alguns momentos, um termo for empregado em letras maiúsculas e outro em minúsculas, é porque, no texto em discussão naquele ponto, o termo é empregado em letras maiúsculas; vale o mesmo para o emprego de siglas.

[2] Nesse caso, com duas perspectivas distintas: uma como sinônimo de "guerra de informações"; e outro, menos frequente, como caracterização de como seria a guerra contemporânea, por contraste a, por exemplo, "guerra industrial" (cf. GILLAN et al., 2008).

Segundo, alguns autores referem-se a algumas ideias como "*war*" (por exemplo, *information war)* e outros como "*warfare*", uma distinção que nem sempre é feita em português; neste texto, "*war*" será traduzido como "guerra", e "*warfare*" como "guerrear". Terceiro, o emprego dos termos nesse texto, com ou sem aspas, em nenhum momento significa qualquer tipo de concordância ou endosso, por parte deste autor, com relação a sua pertinência, validade, adequação ou utilidade para representar ideias, e nem mesmo que essas ideias sejam válidas. Pelo contrário, por exemplo, este autor considera, a partir de Clausewitz, que a guerra é uma ação de força para obrigar o oponente a fazer a nossa vontade – força entendida aqui como força física –, e guerrear é simplesmente executar atividades características, próprias, da guerra; se não há emprego de força física, não há que designar-se uma atividade como "guerra" ou como "guerrear", por mais importante que essa atividade possa ser no contexto. Do mesmo modo, este autor considera inadequado compartimentar a guerra por tipo de espaço, por domínio, por atividade, pois guerrear, em princípio, pode envolver todos esses ambientes e domínios. Por fim, na medida do possível, o emprego dos termos será consistente com o jargão frequentemente empregado pelas forças, como expressos no Glossário das Forças Armadas (BRASIL, 2015), exceto quando se julgar que o emprego do termo pode ser teoricamente inconsistente.

Um esclarecimento adicional: a expressão "ambiente informacional" é empregada em muitos contextos distintos (p. ex., GREIF, 2017; YU; WEBB, 2017; SCHUDSON, 1993); entretanto, ater-se-á aqui a seu emprego (e de outros termos correlatos) no contexto das relações entre atores políticos no ambiente internacional.

2 OS PRIMEIROS ANOS: DA DÉCADA DE 1990 A MEADOS DA DÉCADA DE 2010

Escrevendo em 1995, Martin Libicki (1995), num texto amplamente citado, procurou fazer um balanço da literatura existente até então sobre o tema. No seu entender, não existia um guerrear informacional como atividade distinta, mas sim sete formas diferentes de guerrear informacional, cada uma reivindicando para si o rótulo de "guerrear informacional":

> (i) guerrear de comando-e-controle (que visa a atingir a cabeça e o pescoço do inimigo), (ii) guerrear baseado em inteligência (que consiste na concepção, proteção e negação de sistemas que buscam conhecimento suficiente para dominar o espaço de batalha), (iii) guerrear eletrônico (técnicas radioeletrônicas ou criptográficas), (iv) guerrear psicológico (em que a informação é empregada para mudar as mentes de amigos, neutros e inimigos), (v) guerrear "de *hacker*" (em que sistemas de computadores são atacados), (vi) guerrear de informação econômica (bloquear ou canalizar informação em busca de dominância econômica), e (vii) guerrear cibernético (uma sacola de supermercado de cenários futurísticos). (LIBICKI, 1995, x).

Cada uma dessas formas incluía, em seu entender, subcategorias de atividades. Além disso, essas atividades (bem como algumas das subcategorias) apresentavam, entre si, graus distintos de amadurecimento. Na sua avaliação, todo esse conjunto de atividades que disputavam então o rótulo de "guerrear informacional" era menos problemático do que pareceria à primeira vista. Conclui, então, entre outras coisas, que, embora sistemas de informação tivessem se tornado mais importantes, várias técnicas e procedimentos seriam suficientes para garantir sua integridade: atividades como "bloqueios de informação" e "guerrear cibernético" seriam ainda bastante incipientes, nocionais, e a que ele chama de "guerrear de *hacker"* (que distinguia, então, de guerrear cibernético), embora mais

desenvolvida, à época, seria muito exagerada como "elemento da guerra". Um aspecto interessante é que a ideia de "ambiente informacional" não aparece nenhuma vez no texto; no que concerne ao novo elemento trazido pelos "sistemas de informação", a "arquitetura de informação" é que tinha o maior destaque – revelando uma ênfase muito maior com a infraestrutura do que com os processos, impactos e efeitos, em indivíduos, grupos e sociedades, das atividades informacionais propriamente ditas. De fato, esse entendimento era bastante consistente com a direção geral da discussão, à época. Com efeito, o texto amplamente reconhecido (cf. BLANNIN, 2021) como o primeiro a empregar a ideia de "guerra informacional" focava-se precisamente nos sistemas de circulação de informação:

> A partir da ideia relativamente simples de negar ao oponente a informação necessária para o emprego eficiente de seus armamentos, o progresso no desenvolvimento de contramedidas foi tão rápido que tornou agora possível explorar o conceito mais amplo de fluxo de informações, na medida em que este afeta não apenas o resultado detalhado do engajamento terminal, mas também as escolhas estratégicas e os movimentos táticos que levam àquele engajamento. A ideia de degradar o fluxo de informações do oponente e, por outro lado, proteger o nosso próprio, vem sendo amplamente aceita, e resultou em importantes aplicações. A necessidade de um exame sistemático das consequências previsíveis dessa "guerra informacional" já vem sendo sentida há algum tempo. (RONA, 1976, p. 5).

Também nesse texto, a ideia de "ambiente informacional" ainda não aparece.

Na mesma época, a ambiguidade apontada por Libicki (1995) começa a ser encaminhada na direção de uma maior preocupação com a infraestrutura de comunicação como o centro do guerrear informacional. Por exemplo, num documento produzido pelo Conselho Científico do Exército dos EUA (*US Army Science Board), publicado em 1995, lê-se:*

> Guerrear informacional (ou operações de informação) é a sequência de ações empreendidas por todas as partes em um conflito para destruir, degradar e explorar os sistemas de informação de seus adversários. Por outro lado, o guerrear informacional também inclui todas as ações voltadas para proteger sistemas de informação contra tentativas hostis de destruição, degradação e exploração. O guerrear informacional ocorre ao longo de todas as etapas da evolução de um conflito: paz, crise, escalada, guerra, desescalada e pós-conflito. (US ARMY SCIENCE BOARD, 1995, p. 29, tradução livre).

A convergência com o entendimento de Rona (1976), citado anteriormente, é notória e proposital: Thomas Rona é um dos autores do estudo, e a fonte da citação é referida a uma apresentação sua para a equipe que produziu o relatório. Não há referência ainda, nesse texto, a "ambiente informacional".

Esse entendimento de guerrear informacional foi incorporado doutrinariamente nos EUA. Por exemplo, no antigo Manual de Campanha 100-6 (FM 100-6)[3] *Information Operations*, o guerrear informacional era definido como:

> Ações tomadas para obter superioridade informacional afetando a informação, os processos baseados em informação, sistemas de informação e redes baseadas em computadores do adversário, ao mesmo tempo defendendo os próprios: informação, processos baseados em informação, sistemas de informação e redes baseadas em computadores. (FM 100-6, 1996, p. 2-2, tradução livre).

[3] Por economia de espaço, os documentos doutrinários serão citados no texto pela sua sigla e numeração.

Nessa publicação, já aparece a ideia de "ambiente informacional", mas relacionada ao entendimento de guerrear informacional ali contido, ou seja, ainda fortemente associada a sistemas de informação, e não a seus potenciais efeitos e empregos. O ambiente informacional também aparece de dois modos distintos: o "ambiente informacional global" (GIE) e o "ambiente informacional militar" (MIE):

> O *ambiente informacional global* inclui: todos os indivíduos, organizações ou sistemas – cuja maioria está fora do controle militar ou das Autoridades Nacionais de Comando – que coletam, processam e disseminam informação para audiências nacionais e internacionais. [...]. (FM 100-6, 1996, p. 1-2, tradução livre).
> A esfera de atividade informacional chamada *ambiente informacional militar* é entendida como: o ambiente contido no GIE [nota ED: *Global Information Environment*], e consistem em sistemas de informação (INFOSYS) e organizações – amigas e adversas, militares e não militares, que apoiam, viabilizam, ou influenciam significativamente uma operação militar específica. (FM 100-6, 1996, p. 1-4, tradução livre, grifos no original).

Em que pese o reconhecimento, no documento, de que vários agentes públicos e privados, inclusive pessoas físicas, compunham esse GIE, o FM 100-6 dá especial destaque para o que, no Brasil, é chamado genericamente de "imprensa" (em inglês, *news media*), cuja capacidade de "coletar, processar e disseminar informação" estaria crescendo exponencialmente, ainda de acordo com o documento:

> Claramente, o efeito da informação escrita e, principalmente, da visual trazidas pelas organizações de notícias dos EUA e internacionais influenciou, direta e rapidamente, a natureza dos objetivos de política dos EUA e internacionais, bem como nosso uso de força militar, em Ruanda, na Somália e na antiga república iugoslava. (FM 100-6, 1996, p. 1-3, tradução livre).

Reconhecendo a crescente importância das redes de computadores, o FM 100-6 identifica a existência de três tipos, fortemente interligados, de infraestruturas informacionais:

a. a Infraestrutura Informacional Global (GII), caracterizada como uma "interconexão de redes de comunicações, computadores, bases de dados e bens eletrônicos de consumo *[consumer electronics]* que torna disponíveis, nas pontas dos dedos dos usuários, vastas quantidades de informação" (p. 1-3);

b. as Infraestruturas Informacionais Nacionais (NIIs) de todos os países seriam partes integrantes da GII, e seriam compostas pelos mesmos tipos de elementos dessa última, mas em escala reduzida; e

c. a Infraestrutura Informacional de Defesa (DII), que, no âmbito do Departamento de Defesa (DoD) dos EUA, "conecta os usuários e os computadores de apoio a missões, comando e controle (C2) e inteligência por meio de serviços de voz, imagens a partir de dados [*data imagery*], vídeo e multimídia" (p. 1-4).

Diversos desafios à condução de operações militares estariam relacionados ao GIE: a segurança das informações (*INFOSEC*) que trafegam nesse ambiente; a necessidade de atuação contínua no âmbito do MIE; o impacto que a grande visibilidade das operações militares, incluindo imagens, vídeos e análises de especialistas, pode ter sobre a opinião pública e sobre as decisões políticas e, por decorrência, no próprio moral (*morale*) dos efetivos; e, por fim, as diversas considerações legais – incluindo aspectos ainda não regulamentados, em função de sua novidade – que incidiriam sobre

as operações informacionais (FM 100-6, 1996, p. 1-7 -1-9). Esses desafios podem ser enfrentados, segundo o FM 100-6, por meio da "dominância informacional", definida como:

> O grau de superioridade informacional que permite a seu possuidor usar sistemas e capacidades informacionais para obter vantagem operacional em um conflito ou controlar a situação em operações em intenso conflito sem que haja guerra [*operations short of war*], ao mesmo tempo negando essas capacidades ao adversário. (FM 100-6, 1996, p. 1-9).

De acordo com o FM 100-6, entende-se a importância da dominância informacional para as operações militares como semelhante à importância de superioridade aérea. A dominância informacional tem dois aspectos igualmente importantes: construir e proteger as capacidades informacionais amigas; e degradar as capacidades informacionais inimigas. A ideia é que o conhecimento e o entendimento da situação devem ser "mais certos, mais oportunos, e mais precisos que os do adversário, revelando ao comandante amigo as condições que levarão ao sucesso" (FM 100-6, 1996, p. 1-9). A dominância informacional seria obtida, então, pelo guerrear informacional, ou seja, pela execução de operações informacionais (IO). Estas, por sua vez, são definidas como:

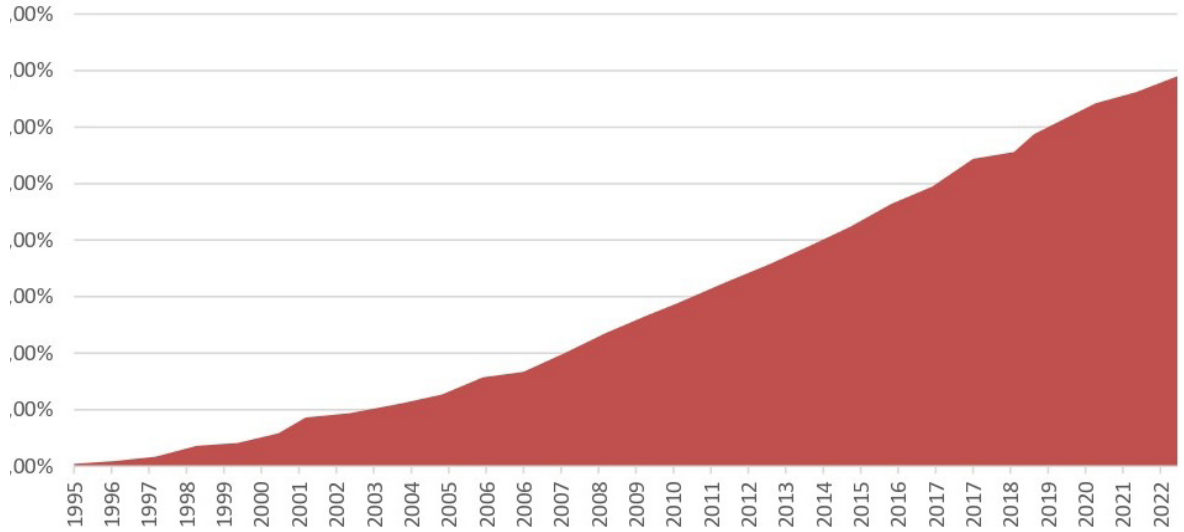
> Operações militares contínuas no interior do MIE que viabilizam, ampliam e protegem a capacidade das forças amigas de coletar, processar, e agir a partir de informações de modo a obter vantagem ao longo de todo o leque de operações militares; IO incluem interagir com o GIE e explorar ou negar capacidades de informação e de decisão de um adversário. (FM 100-6, 1996, p. 2-3).

Nessa concepção de ambiente informacional, as operações informacionais seriam: as operações de guerrear de comando-e-controle (C^2W) ofensivas e defensivas, cujos propósitos são "influenciar, negar informação a, degradar ou destruir as capacidades de C^2 do adversário, protegendo as capacidades de C^2 próprias" (p. 2-4); operações de assuntos civis (CA), voltadas para "estabelecer, manter, influenciar ou explorar relações entre forças militares, autoridades civis e a população civil numa AO (Área de Operações), de modo a facilitar a execução de operações militares" (p. 2-5); e operações de comunicação social (Public Affairs Operations, PA), voltadas para o monitoramento de percepções públicas e para a elaboração e disseminação de mensagens claras e objetivos sobre as operações militares (p. 2-5).

Assim, no que concerne ao entendimento do ambiente informacional e de como atuar nele e a partir dele, o FM 100-6 reflete um mundo em que a capacidade de produção e disseminação de conteúdo por indivíduos ainda era, de certa forma, limitada, em função do baixo acesso relativo das pessoas à Internet (Gráfico 1). Havia, então, ou parecia haver, em situações de conflito mais intenso, uma ampla capacidade de atuação para forças armadas no sentido de, tanto agindo diretamente, quanto por meio de atuação junto à grande imprensa – de longe, à época, a principal provedora de conteúdo informacional – e a governos e outras organizações, tentar influenciar as ações, decisões e estado psicológico de comandantes, lideranças e populações dos adversários, dos aliados e próprias.

Entretanto, o fato de que, quando o FM 100-6 foi publicado, em 1996, menos de 0,5% da população mundial tinha acesso à Internet não altera o fato de que alguns desses usuários eram capazes de explorar diversas vulnerabilidades, ao passo que a imensa maioria dos usuários – inclusive em organizações militares – e várias das organizações que tinham acesso à rede não tinham qualificação nem recursos para fazer frente a essas ações hostis. A atenção dada, tanto na FM 100-6 quanto em outras publicações da época – por exemplo, no texto de Libicki (1995), já mencionado – à infraestrutura e aos sistemas de informação é consistente com essa realidade.

Gráfico 1 - Número de usuários da Internet como porcentagem da população mundial (1995-2022)



Fonte: Elaborado pelo autor, a partir de https://www.internetworldstats.com/emarketing.htm

Na mesma direção, um estudo pioneiro da Rand Corporation (MOLANDER et al., 1996), embora reconhecendo que a noção de “guerrear informacional” ainda permaneceria um tanto vaga por algum tempo, definia o “guerrear informacional estratégico” como um “campo [realm] emergente de conflito em que nações utilizam o ciberespaço de modo a afetar operações militares estratégicas e infligir dano em infraestruturas informacionais nacionais” (MOLANDER et al., 1996, p. 1), sendo que o ciberespaço é entendido ali como a GII, como no FM 100-6. Consistentemente com aquela visão do ambiente informacional em que o ciberespaço permitiria a indivíduos prejudicar a realização de atividades relevantes em caso de guerra, esse estudo da Rand Corporation identifica, como um dos atributos definidores do guerrear informacional estratégico o fato de que os custos de entrada seriam baixos (*low entry cost*). Por outro lado, identificando a tendência de que a quantidade de pessoas com acesso à Internet iria aumentar significativamente, os autores do estudo consideraram que um outro atributo definidor do guerrear informacional estratégico seriam as possibilidades: (i) de divulgação de notícias e mensagens sem a intermediação de organizações como as empresas jornalísticas ou serviços de entrega; e (ii) de produção e divulgação de falsificações, com o intuito de manipular percepções, atitudes e decisões. Portanto, essa possibilidade abriria amplo espaço para atividades de “gestão da percepção” (*perception management*), tanto ofensivas (atuar sobre a percepção do oponente – forças, comando, lideranças, população) quanto defensivas (atuar sobre a percepção das audiências próprias) (MOLANDER et al., 1996, p. 15-24). Assim, embora, nesse estudo, o foco ainda recaia principalmente sobre a possibilidade de atividades no ciberespaço, observa-se já alguma atenção a atividades voltadas diretamente para efeitos cognitivos.

Essa percepção, contudo, não transparece na publicação que sucede ao FM 100-6, que é o FM 3-13[4] –, publicado em 2003. Neste, a ideia de ambiente informacional é bastante semelhante à contida no FM 100-6 de 1996, mas com uma ênfase ainda maior nas atividades relacionadas ao ciberespaço – possivelmente refletindo o drástico aumento, no período entre as duas publicações,

[4] Entre uma e outra, houve a mudança no sistema de categorização das publicações doutrinárias nos EUA, inclusive no Exército dos EUA.

da população mundial com acesso à Internet (de 0,4% em 1995 a 9,4% em 2002 – uma média de crescimento de 62,65% ao ano). A distinção entre os ambientes informacionais global, nacionais e de defesa já não aparece, e a GII é basicamente redefinida como a "Malha Informacional Global" (*Global Informational Grid*, GIG), mas o ambiente informacional é definido como "... o agregado de indivíduos, organizações ou sistemas que coletam, processam ou disseminam informações; dele faz parte também a própria informação" (FM 3-13/2003, p. 1-2). O ambiente informacional incluiria "a interconexão de redes de comunicações de alcance global"; os "sistemas de comando-e-controle (C^2) de forças e outras organizações amigas e adversárias"; "pessoal amigo, adversário e outros, que tomam decisões e manuseiam informação" (FM 3-13/2003, p. 1-2). Notoriamente, afirma-se, na publicação, que "ameaças baseadas no ambiente informacional visam a um de três objetos: comandantes e outros tomadores de decisão importantes, sistemas de C^2, ou sistemas de informação (*INFOSYS*)" (FM 3-13/2003, p. 1-3). De modo igualmente significativo, os métodos de ataque próprios ao ambiente informacional identificados pelo FM 3-13/2003 são: acesso não autorizado; *softwares* maliciosos; despistamento eletromagnético; ataque eletrônico; destruição física de sistemas de C2; e gestão da percepção (FM 3-13/2003, p. 1-6 - 1-8). Apenas a última, refletindo elementos então novos, trazidos pela literatura especializada da época, relaciona-se a aspectos cognitivos, mas enfatizando, ainda, a relação com as empresas jornalísticas como principais veiculadores de informação, incluindo propaganda, despistamento e operações psicológicas (PSYOPS). No FM 3-13/2003, não há qualquer menção a "guerra informacional" por si[5], nem a "dominância informacional"[6].

A discussão sobre o ambiente informacional no contexto da guerra tornou-se mais sofisticada depois disso. Gillan, Pickerill e Webster (2008) sustentaram que a "guerra informacional" teria uma faceta sólida, material (*hard side*), a dos armamentos, mas que estes estariam amplamente digitalizados, na qual os EUA tinham ampla liderança; por outro lado, teria também uma faceta intangível (*soft side*), caracterizada pelo ambiente informacional[7] modificado, próprio da primeira década do Século XXI, em que as guerras ocorreriam. Segundo eles, esse ambiente informacional teria as seguintes características:

a. uma esfera de comunicações e de mídia significativamente aumentada pela transmissão por satélite e cabo, incluindo canais de notícias 24/7, existentes em diversos países, e pela Internet;

b. em decorrência, ter-se-ia tornado muito difícil o controle da informação por parte de governos e das forças armadas;

c. especialmente difícil de controlar seria a informação enviada por repórteres, graças à digitalização das imagens, às câmeras portáteis, inclusive as de celular, e os serviços e acesso à Internet pelas redes de serviços de telefonia móvel;

d. um entendimento amplamente disseminado de que cidadãos em democracias têm direito de saber o que estaria sendo feito "em seu nome"; e

[5] A expressão só aparece quando o texto se refere a uma antiga designação, que já não vigia: "*Field support teams from the 1st Information Operations Command (Land) (1st IOC [L]), formerly known as the Land Information Warfare Activity (LIWA), can assist in this effort (see appendix F).*" (FM 3-13/2003, p. 3-4).

[6] A única menção à expressão *information dominance* é em um apêndice, em referência a uma instância específica: "*INSCOM's IO capabilities focuses around the Information Dominance Center (IDC).*" (FM 3-13/2003, p. F-19).

[7] Seu entendimento é explicitamente inspirado no estudo clássico de Schudson (1993 – publicado pela primeira vez em 1984) sobre a indústria da publicidade. Mais adiante, ao analisar-se a caracterização da atual "infosfera" (MAZAR et al., 2019), far-se-ão novas referências a esse estudo extraordinário.

e. finalmente, "[…] esse ambiente informacional significa que os civis, embora não tenham sido chamados a ter experiência direta da guerra como soldados no terreno ou reservas, têm uma experiência mediada da guerra enormemente expandida [...]. Esta é uma experiência a distância que é também notoriamente próxima [...], a partir da televisão ou do monitor do PC." (GILLAN et al., 2008, p. 1836, tradução livre, grifo no original)[8]. Sobre isso, os autores comentam: "Ainda assim, trata-se de um fenômeno notável: embora nossos pais e avós tenham frequentemente tido experiência direta de conflitos, hoje, nós temos muito mais conhecimento da guerra, mas basicamente de longe. Nós estamos mais protegidos da guerra que nunca; ainda assim nós a testemunhamos, frequentemente com detalhes estarrecedores, como espectadores." (id., ibid.).

Nessa perspectiva, uma atividade central da "Guerra Informacional" seria a gestão de percepções (perception management), que seria realizada mediante a "gestão da informação". Nenhuma das duas atividades é definida explicitamente no texto, mas fica claro que a perspectiva de Gillan, Pickerill e Webster (2008) é centrada na faceta intangível da "Guerra Informacional" conduzida por democracias – que dependem, em muito maior medida que governos não democráticos, do apoio popular para a continuidade das atividades na guerra –, para seu público interno e/ou dos aliados; entretanto, nada há no entendimento exposto no texto que seja incompatível com seu emprego junto aos públicos de Estados neutros ou hostis. Essa gestão da informação seria realizada mediante diversas tarefas, desde treinar oficiais em como lidar com a mídia até a seleção de jornalistas que acompanhariam as forças próximas ao desenrolar das hostilidades. Cabe lembrar que, apesar de reconhecerem a importância da Internet, os autores têm em mente um mundo em que as grandes empresas jornalísticas tiveram sua centralidade aumentada, em função dos canais de notícias em 24 horas das TVs por assinatura, e em que plataformas de redes sociais virtuais como Twitter, Facebook e YouTube apenas começavam a ganhar espaço[9], processo que se acelera com o lançamento do iPhone® para sistemas 3G e dos *smartphones* com sistema operacional Android®, ambos em 2008[10].

Mesmo assim, Gillan, Pickerill e Webster (2008) chamam a atenção para o fato de que, já naquelas condições, dada a caracterização do ambiente informacional feita por eles, o exercício da gestão de percepções mediante a gestão da informação – a que eles se referem como o "modelo do controle de informação sobre a guerra" – seria impraticável. Para os autores, as pesquisas quantitativas que apontavam que a cobertura jornalística e midiática sobre as guerras priorizava significativamente fontes militares e governamentais, concluindo que aquela cobertura seria desproporcionalmente influenciada por esse tipo de fontes, simplesmente não levavam em conta aspectos cruciais: (i) a diferença de importância relativa das histórias – por exemplo, histórias que mostram, eventualmente com imagens, soldados capturados pelo oponente ou civis mortos por erros ou descuidos teriam um impacto muito maior junto ao público do que a maioria das informações transmitidas por fontes oficiais; (ii) o impacto desproporcional que determinados eventos podem ter – como renúncias de autoridades em protesto contra decisões, ou erros muito significativos. Mas, para os autores, a principal crítica ao modelo do controle de informações sobre a guerra é que ele seria obsoleto, em função do caráter

[8] As elipses, nessa citação, excluem apenas algumas referências bibliográficas presentes no texto, que não faz sentido citar aqui.

[9] Ver o gráfico disponível em https://ourworldindata.org/images/published/social-media-users-over-time_850.webp para a evolução do número de usuários de diversas mídias sociais.

[10] No gráfico mencionado na nota anterior, fica nítido o salto no número de usuários de plataformas de redes sociais virtuais a partir de 2008.

"caótico e certamente mais confuso e ambíguo" do ambiente informacional da guerra contemporâneo (GILLAN; PICKERILL; WEBSTER, 2008, p. 1837-1839).

O artigo de Gillan, Pickerill e Webster (2008) ilustra bem a evolução da discussão acerca das mudanças nos processos sociais de produção, armazenamento, processamento e disseminação da informação na sociedade contemporânea e das condições pelas quais as percepções, e consequentemente as decisões, de indivíduos, lideranças, grupos e sociedades podem ou não ser afetadas intencionalmente, e em que medida. Mas, como salientado anteriormente, ele ainda não capta três dos principais fenômenos que afetariam significativamente os processos sociais da informação: a ampliação do acesso à Internet pelos serviços de telefonia móvel; o surgimento do iPhone® para sistemas 3G e dos *smartphones* com sistema operacional Android®; e a disseminação do uso de plataformas de redes sociais virtuais.

O resultado combinado desses fenômenos mudou drasticamente o contexto social do ciclo da informação[11]. O conteúdo que circula nessas plataformas tem duas características muito importantes: audiências potenciais muitas vezes maiores que as das grandes empresas jornalísticas tradicionais, inclusive redes de televisão; e o custo de produção dessa informação, para as empresas que gerem as plataformas, é insignificante, no sentido mais extremo da palavra, pois o conteúdo produzido por elas mesmas é mínimo – os usuários é que o produzem, ou então disseminam nas plataformas o conteúdo produzido por outrem, com destaque para o conteúdo produzido pelas empresas jornalísticas, reproduzido integral ou parcialmente, ou ainda parafraseado pelos autores das mensagens. Com isso, declinou drasticamente o benefício a ser obtido comprando na banca ou assinando, ainda que digitalmente, serviços jornalísticos (ou mesmo do tempo dedicado a assistir aos noticiários das TVs abertas e por assinatura), o que levou a uma diminuição igualmente drástica do benefício a ser obtido por anunciantes, reduzindo enormemente a receita publicitária das empresas jornalísticas e fazendo subir o custo fixo por leitor/telespectador da produção da notícia – o que gera desincentivos adicionais à aquisição de produtos e serviços jornalísticos, reforçando o círculo vicioso.

Paradoxalmente, o acesso de leitores às notícias produzidas (condição necessária para que as empresas jornalísticas obtenham alguma receita com anúncios, na Internet) passou a depender de produzirem interesse suficiente para que alguém as divulgue nas plataformas de redes sociais virtuais e para que quem seja alcançado pelas postagens queira acessar a página original: "Isso significa que, para os veículos de notícias, sua viabilidade depende de identificar sua claque e agradá-la; jogar para a torcida, como se diz" (DINIZ, 2021). Como as situações de leitura e acesso às mensagens divulgadas nessas plataformas são muito diferentes das condições em que jornais e revistas semanais eram lidos e em que se assistia a programas jornalísticos das emissoras de TV, as notícias tiveram que se adaptar às condições bem mais casuais, mais frequentes e com duração e atenção mínimas por parte dos leitores as consomem. Houve, então, uma pressão para a rápida e constante produção de notícias muito curtas – com menos tempo disponível para checagem e confirmação, e com menos contexto, reflexão e diversidade de perspectivas em cada publicação; e a necessidade concomitante de redução de custos. Escritórios regionais e no exterior tiveram que ser fechados, o que tornou a cobertura de assuntos que não fossem locais drasticamente reduzida e baseada cada vez mais em conteúdo produzido por outrem. Com isso, claramente, caíram a qualidade e a utilidade das notícias.

O decréscimo da quantidade de notícias de qualidade atingiu severamente a credibilidade

[11] Este parágrafo e o seguinte expõem, de maneira condensada, a descrição feita em outro texto (DINIZ, 2021). Remete-se o leitor a este, para mais detalhes e para outras referências.

das empresas jornalísticas, o que fez com quea credibilidade relativa de outras fontes, quaisquer que fossem, aumentasse. Como, principalmente nas plataformas de redes sociais virtuais – mas também em *blogs* e outros tipos de mídia disponíveis para qualquer um, a custo baixíssimo, na Internet –, a quantidade de produtores (e copiadores e disseminadores) de conteúdo cresceu exponencialmente, os processos sociais de circulação da informação se tornaram cacofônicos, ainda mais caóticos do que aqueles caracterizados por Gillan; Pickerill; Webster (2008). Com isso, aumentou significativamente a demanda social por motores de busca na Internet. Um aspecto importante dessa nova realidade social dos processos informacionais é que mensagens elaboradas com uma determinada audiência em mente podem, e quase sempre vão, atingir audiências diferentes, em contextos sociais marcadamente diferentes, e poderão ser interpretadas de (múltiplos) modos, bastante diferentes da intenção que seu autor original tinha em mente.

Para completar, a vastidão de informações que os usuários das plataformas de redes sociais virtuais disponibilizam a estas, voluntária e gratuitamente, quando processadas por meio de inteligência artificial, torna possível um grau de segmentação do público que seria inimaginável para as empresas jornalísticas tradicionais, permitindo que os anúncios veiculados sejam dirigidos quase exclusivamente aos potenciais interessados nos produtos e serviços anunciados, sem o grau de desperdício (ou seja, de pessoas alcançadas que não são potenciais compradores, por desinteresse ou por falta de recursos) característico de um comercial de 30 segundos no horário nobre da TV aberta. Como o custo por usuário das grandes plataformas de redes sociais virtuais e dos grandes motores de busca é mínimo, assim como é mínimo o desperdício de cada anúncio, a verba publicitária se dirige cada vez mais a esses veículos, intensificando a pressão sobre a receita das empresas jornalísticas tradicionais e, novamente, aumentando os efeitos do ciclo vicioso descrito anteriormente. Com efeito: em 2020, a Alphabet (controladora do Google e do YouTube) ficou com 29,7%, a então chamada Facebook (controladora do Facebook, do Instagram e do WhatsApp) com 23,5% e a Amazon com 10,2% do mercado publicitário dos EUA – onde estão, entre outros, o New York Times, o Washington Post, a CNN, a Fox News, o USA Today... Ou seja, apenas três empresas abocanharam quase dois terços do maior mercado publicitário do mundo.

O Manual de Campanha FM 3-13 de 2013, que substituiu o FM 3-13/2003, refletiu em grande medida essas mudanças sociais e o deslocamento, na literatura, da ênfase sobre os sistemas para os aspectos cognitivos na discussão sobre o guerrear informacional. Sintomaticamente, o FM 3-13/2013 não é mais designado como *Information Operations*, mas sim como *Inform and Influence Activities* (Atividades de Informar e de Influência)[12]. Aqui, a definição de ambiente informacional começa exatamente do mesmo modo que na versão anterior: "*[...]* o agregado de indivíduos, organizações ou sistemas que coletam, processam ou disseminam informações". Contudo, em seguida, a diferença começa a aparecer: "Conceitualmente, o ambiente informacional abrange tanto elementos tangíveis (físicos) quanto intangíveis (como as ideias, medos, percepções e tomada de decisões humanos" (FM 3-13/2013, p. 2-2, tradução livre). Esse ambiente seria constituído pelas dimensões física, informacional e cognitiva:

a. a dimensão física seria composta por "elementos tangíveis como redes de telecomunicações, sistemas e infraestruturas de informações, satélites, instalações de emissoras [de rádio e televisão], pontos de encontro, publicações impressas, instalações para cartazes (*billboards*),

[12] Na versão de 2016, que substituiu a de 2013, o FM 3-13 voltou a ser designado como *Information Operations*.

panfletos, estátuas, objetos simbólicos, organizações, grupos e pessoas" – incluindo também as faixas de transmissão do espectro eletromagnético, que não são, literalmente, tangíveis –, ou seja, os meios e métodos que "viabilizam o fluxo de informação entre produtores, usuários, audiências, e sistemas" (FM 3-13/2013, p. 2-2, tradução livre);

b. a dimensão informacional incluiria "a própria informação, seja estática (no repouso) ou em trânsito", e referir-se-ia "ao conteúdo e ao fluxo da informação, como textos, ou imagens, ou dados que os servidores possam coletar, processar, armazenar, difundir e exibir", provendo assim "a conexão necessária entre a dimensão física e a dimensão cognitiva" (FM 3-13/2013, p. 2-2, tradução livre); e

c. a dimensão cognitiva seria constituída pelos "valores, crenças, conceitos, intenções e percepções de indivíduos e grupos que transmitem e recebem informações"; nessa dimensão, "tomadores de decisões de públicos-alvos estão maximamente suscetíveis à gestão da influência e da percepção". (FM 3-13/2013, p. 2-2 - 2-3, tradução livre).

O FM 3-13/2013 também reflete, parcialmente, o entendimento de que é muito difícil, nas atuais condições, influenciar percepções por meio do controle sobre a produção e circulação de informações. A "linha de esforços de informes" das Atividades de Informes e Influência (IIA) focar-se-ia em "prover mensagens de informação para audiências domésticas e globais que descrevam com veracidade [*accurately*] a execução de operações ou prover informações pertinentes para audiências específicas numa área de operações"; nesse caso, não se trataria de "forçar um ponto de vista particular sobre audiências, mas sim de fornecer-lhes fatos de modo a que elas possam aumentar seu conhecimento ou tomar suas próprias decisões. Prover informação crível, fatual, e verídica funciona com o melhor meio de confrontar informações falsas ou enganosas disseminadas por outros esforços informacionais" (FM 3-13/2013, p. 2-1, tradução livre). Esse mesmo ceticismo salutar quanto à eficácia das tentativas de influenciar percepções e comportamentos por meio da manipulação de informações, contudo, não se estende da mesma maneira à "linha de esforços de influência", voltada para "mudar atitudes e comportamento de audiências externas neutras, contrárias e inimigas, em apoio à obtenção dos objetivos de área conjunta de operações", como, por exemplo, "produzir falsas impressões [*misleading*] nos tomadores de decisões do inimigo ou convencer forças inimigas a se renderem" (FM 3-13/2013, p. 2-2, tradução livre).

O FM 3-13/2013 dá importância destacada à comunicação estratégica e às operações informacionais. A primeira passa a ser entendida como "os esforços do Governo dos Estados Unidos em entender e engajar audiências-chaves para criar, fortalecer ou preservar condições favoráveis para o avanço em direção aos interesses, políticas e objetivos do Governo dos Estados Unidos por meio do emprego coordenado de programas, planos, temas, mensagens e produtos, sincronizadamente com as ações de todos os instrumentos do poder nacional" (FM 3-13/2013, p. 2-4, tradução livre). Por sua vez, as operações informacionais são redefinidas como "o emprego integrado, durante operações militares, de capacidades relacionadas à informação, concertadamente com outras linhas de operações, para influenciar, perturbar de modo a interromper [*disrupt*], danificar severamente [*corrupt*] ou usurpar a tomada de decisão de adversários atuais e potenciais e, ao mesmo tempo, proteger os próprios" (FM 3-13/2013, p. 2-4, tradução livre).

Embora, no documento, reconheça-se que, em princípio, qualquer atividade ou capacidade tenha conteúdo informacional e, de certo modo, transmita uma mensagem - um ponto particularmente destacado em Schwille et al. (2021) -, as seguintes capacidades relacionadas à informação (*information-related capabilities, IRCs) seriam regularmente empregadas nos esforços de IIA:*

a. comunicação social (*public affairs*);

b. "operações militares de apoio informacional" ou MISO[13];

c. engajamento de soldados e líderes, genericamente identificados como "interações entre soldados, líderes e audiências na área de operações";

d. câmeras de combate;

e. operações de assuntos civis;

f. considerações civis e culturais;

g. segurança operacional; e

h. despistamento militar (FM 3-13/2013, p. 3-1, tradução livre).

Já as capacidades que apoiariam as IIA seriam:

a. atividades cibernéticas e eletromagnéticas, incluindo:
- o guerrear eletrônico,
- operações no ciberespaço,
- operações de gestão do espectro eletromagnético;

b. operações técnicas especiais;

c. "presença, postura e perfil"[14];

d. ataque físico; e

e. segurança física (FM 3-13/2013, p. 3-1, tradução livre).

Essa caracterização mostra claramente a mudança no entendimento e na caracterização do ambiente informacional, para o Exército dos EUA, e o consequente deslocamento do foco dos sistemas informacionais para os efeitos desejados em termos de percepções, atitudes, comportamentos e decisões.

Em linhas gerais, esses entendimentos são mantidos na versão atualmente vigente do FM 3-13 do Exército dos EUA, que é a de 2016. As duas únicas mudanças conceitualmente significativas são: (i) a expressão "Atividades de Informes e de Influência" é retirada[15] – o FM 3-13/206 volta a chamar-se *Operações Informacionais*, embora acrescido do subtítulo "Doutrina, Tática, Técnicas e Procedimentos" – e, consequentemente, não há mais referência às duas "linhas de esforços" de Informes e de Influência; (ii) a "comunicação estratégica" desaparece do documento. As definições de "ambiente informacional" e de "operações informacionais" são basicamente as mesmas constantes no FM 3-13/2013, assim como os efeitos desejados associados a essas últimas, mas com uma discreta mudança, enfatizando ainda mais o foco sobre seus aspectos cognitivos:

> Os efeitos imediatos [das operações informacionais] (perturbar de modo a interromper [*disrupt*], danificar severamente [*corrupt*], usurpar) são possíveis nas dimensões física e informacional do ambiente informacional por meio da negação, degradação ou destruição das capacidades relacionadas à informação do inimigo. Entretanto, efeitos na dimensão cognitiva (influenciar) levam mais tempo para se manifestarem. São esses efeitos cognitivos

[13] "Operações militares de apoio informacional", na verdade, seriam as antigas "operações psicológicas" ou PSYOPS, rebatizadas para salientar o compromisso com a veracidade das informações divulgadas, conforme analisado por, p. ex., Paul (2010).

[14] Designando, respectivamente, *grosso modo*, o tamanho do efetivo na área de operações, a sua atitude (mais discreta ou mais conspícua, mais contida ou mais agressiva, etc.) e a sua composição.

[15] Não nos foi possível identificar o porquê dessa mudança. É surpreendente, entretanto, que a nova versão tenha sido lançada apenas três anos depois da anterior. A primeira hipótese – de que isso decorreria do impacto causado pela anexação da Crimeia pela Rússia, em 2014-2015, que causou tanto impacto na discussão, como se verá a seguir – não parece consistente com o grau de continuidade identificado entre as duas versões.

> – manifestados como mudança de comportamento – que são os mais importantes para a obtenção de resultados decisivos. (FM 3-13/2016, p. 1-4).

Por sua vez, a caracterização das IRCs também sofre discretas modificações, muito menos significativas. As IRCs "inerentemente relacionadas à informação ou focadas primariamente em afetar o ambiente informacional" passaram a incluir: as atividades cibernéticas e eletromagnéticas, o guerrear eletrônico, as operações no ciberespaço e as operações técnicas especiais (que, na versão anterior, eram consideradas IRCs de apoio); e as operações espaciais. Não há mais referência a IRCs de apoio, mas sim a uma "ampla variedade de funções e atividades de unidades" que poderiam contribuir para as operações informacionais. Algumas delas constavam, na versão anterior, entre as IRCs de apoio, mas foram acrescentadas também: a estratégia de comunicações do comandante ou sincronização de comunicações; a divulgação seletiva de informações confidenciais para outros países (*foreign disclosure*); manobras físicas; programas especiais de acesso; operações civis-militares; inteligência; ações destrutivas e letais. "Ataque físico" desaparece da lista.

Assim, a discussão sobre guerra informacional, guerrear informacional, operações informacionais e ambiente informacional parece ter percorrido um longo caminho desde 1995. Refletindo esse fato, o próprio Martin C. Libicki, que, em 1995, arguíra contra a existência de uma ideia coerente de guerrear informacional, num texto de 2017 (LIBICKI, 2017), já considera que há razões para que os vários elementos que, no seu entender, constituíam o guerrear informacional pudessem ser agora considerados "partes de um todo maior":

a. vários dos elementos estariam usando as mesmas técnicas, começando pela "subversão" de computadores, sistemas e redes;

b. como consequência do primeiro, os aspectos estratégicos daqueles elementos também estariam convergindo – todos os elementos do guerrear informacional difeririam das operações cinéticas, e de modo semelhante (ampla variância nos efeitos, baixa letalidade, ambiguidade ou dificuldade de atribuição de autoria, e para qual propósito, e, por fim, maior persistência dos praticantes em função da pequenez de suas unidades, sem equipamento excessivamente dispendioso, volumoso e chamativo); consequentemente, todos esses elementos poderiam ser empregados em operações em que aquelas características sejam úteis, ou em que operações cinéticas sejam inadequadas; e, portanto, em tais circunstâncias, o emprego do elementos do guerrear informacional deveriam ser considerados conjuntamente, e não separadamente; e

c. alguns países – segundo ele, a Rússia e, em menor medida, a Coreia do Norte, o Irã e a China – já estariam integrando os elementos do guerrear informacional.

3 DEPOIS DA ANEXAÇÃO DA CRIMEIA PELA RÚSSIA (2014-2015): NOVO IMPULSO À DISCUSSÃO, "GUERREAR HÍBRIDO" E A "ZONA CINZENTA"

Um acontecimento posterior – ou, melhor dizendo, uma determinada percepção sobre esse acontecimento – causou um terremoto na literatura, que ainda está sendo absorvido por publicações doutrinárias e debatido nas publicações acadêmicas: a anexação da Crimeia pela Rússia, em 2014-2015, e o furor em torno da ideia de "guerrear híbrido" (*hybrid warfare).*

A discussão sobre a concepção de "guerrear híbrido" é imensa, e uma análise detida terá

que ficar para outra ocasião[16]. A rigor, o termo antecede a ação russa na Ucrânia, mas, após esse evento, as publicações sobre o assunto dispararam. Ao longo do tempo, inclusive, o termo ter-se-ia descolado do seu significado original, e a literatura teria, em linhas gerais, convergido no entendimento de que o suposto sucesso estrondoso da Rússia dever-se-ia a uma nova maneira de empregar as operações informacionais, principalmente na "zona cinzenta"[17], e que esse forma de "guerrear informacional" seria o principal elemento do guerrear híbrido. A partir desse entendimento, "o Ocidente" estaria, em 2014, despreparado e incapaz de confrontar o guerrear híbrido russo. Isso levou à Declaração da Cúpula da OTAN no País de Gales, em 2014; à criação do Centro Europeu de Excelência para Confrontar a Guerra Híbrida, em 2017; e, por fim, às diversas propostas sobre como lidar com essa ameaça – o que incluiu um esforço renovado de entendimento do novo ambiente informacional que poderia ser explorado pela Rússia e, em menor medida, pela China. De acordo com esse tipo de entendimento, para confrontar a "guerra híbrida", as campanhas de desinformação ("o modelo 'mangueira de incêndio de falsidades' de propaganda russa", no dizer de Paul e Matthews, 2016) e às campanhas visando a minar a confiança e a coesão dos países interessados em manter a "ordem internacional baseada em regras" (*rule-based international order,* RBIO), seria necessário que estes também se dispusessem a travar essa "guerra híbrida", inclusive abaixo do limiar do conflito armado.

Estudos mais detidos (CALISKAN; CRAMERS, 2018; CALISKAN; LIÉGEOIS, 2020; FABIAN, 2019; GALEOTTI, 2016; JANIČATOVÁ; MLEJNKOV, 2021; KÄIHKÖ, 2021; KILINSKAS, 2016; LIBISELLER, 2023; MUMFORD; CARLUCCI, 2023; RENZ, 2016) demonstraram que, ao contrário do que se afirma, o sucesso da Rússia em 2014 não pode ser creditado às concepções que ficaram associadas à "guerra híbrida", e sim a condições muito específicas que não têm como se repetir; que a prioridade dos esforços de modernização das forças russas concentra-se em aprimorar sua capacidade de infligir dano físico; que os debates doutrinários e estratégicos russos estão muito distantes das concepções de "guerra híbrida" expressas na literatura ocidental – em alguns casos, essas concepções são consideradas, por alguns autores, como propaganda ocidental anti-Rússia; e que não há qualquer evidência de que a estratégia seguida em 2014 esteja consagrada numa concepção mais geral da ação política da Rússia no plano internacional. Para alguns, a concepção de "guerra híbrida", tal como desenvolvida principalmente a partir de 2014 (em que pese a existência de trabalhos anteriores que empregavam o termo, mas com um sentido bastante diferente), refletiria na verdade a surpresa de políticos e acadêmicos, principalmente de Estados-membros da OTAN, com os acontecimentos de 2014.

Não obstante, um dos efeitos dos acontecimentos de 2014-2015 na Ucrânia foi o debate sobre o guerrear híbrido, principalmente como supostamente praticado pela Rússia, e sobre como lidar com ele. Dada a centralidade percebida das atividades relacionadas à informação nessa suposta forma russa de guerrear, uma parte importante do debate foi centrada no guerrear informacional e na caracterização do ambiente informacional. Na discussão a seguir, destacar-se-ão dois aspectos

[16] Alguns bons textos para referência inicial são: Caliskan e Cramers (2018); Caliskan e Liégeois (2020); Fabian (2019); Galeotti (2016); Janičatová e Mlejnkov (2021); Käihkö (2021); Kilinskas (2016); Libiseller (2023); Mumford e Carlucci (2023); Rácz (2015); Renz, 2016; Wither (2016). Sobre como lidar com a "guerra híbrida", sem pretensão de exaustividade, podem-se citar: Blyte e Calhoun (2019); Echevarría (2015); Kramer e Speranza (2017); Paul e Matthews (2016); Schwille et al. (2023) (algumas são tão vagas e inócuas que tornam difícil identificar por que seriam adequadas para lidar especificamente com "guerra híbrida" e operações de informação, e não com qualquer outra situação: p. ex., Marovic, 2019; Fontaine, 2019).

[17] Voltar-se-á à discussão da "zona cinzenta" mais adiante.

do debate que se seguiu: um sobre o novo ambiente informacional, cuja análise mais sofisticada – inclusive bem mais próxima da concepção original, formulada por Schudson (1993 [1984]) –, mas com aspectos problemáticos, feita por Mazarr et al. (2019); e a própria ideia de "zona cinzenta", proposta originalmente pelo próprio Mazarr (2015) e retomada em Morris et al. (2019).

3.1 Caracterizando o ambiente informacional atual

Ao analisar o que chamam de "manipulação social hostil"[18] – "a geração e disseminação sistemáticas de informação para a produção de resultados sociais, políticos e econômicos nocivos num país-alvo ao afetar crenças, atitudes e comportamentos"[19] (MAZARR et al., 2019, p. 1) –, Mazarr et al (2019) sugerem que esta seria facilitada pelas características da atual "infosfera" ou ambiente informacional – os dois termos são considerados basicamente sinônimos no documento –, ou seja, "o processo social em curso de produção, disseminação e percepção da informação numa sociedade" (p. 5). Na sua forma mais extrema, visando a sabotar e manipular as redes informacionais de uma sociedade, a manipulação social hostil se tornaria "guerrear societal virtual". No enfrentamento dessa questão, Mazarr et al. (2019) produziram uma síntese bastante útil e atualizada de vários aspectos relevantes do atual ambiente informacional ou, como preferem os autores, da atual infosfera[20].

No que concerne às tendências mais específicas à própria infosfera, os autores destacam:

a. a dinâmica em redes e o papel da informação viralizada, ou seja, que se espalham ampla e aceleradamente, permitindo que informações de todo tipo, incluindo a possibilidade de que sejam deliberadamente enganosas e voltadas para tentativas de manipulação – e, geralmente, exageradas e chamativas –, cuja viralização tende a reforçar sua reprodução e, frequentemente, até mesmo sua credibilidade junto a alguns públicos;

b. tendência ao sensacionalismo, que, exatamente por exagerar aspectos chamativos de determinadas histórias, tende a facilitar sua propagação – contaminando até mesmo a produção informacional de empresas jornalísticas;

c. a gigantesca multiplicidade de produtores de informação – independentemente de sua qualidade –, ou seja, uma enorme fragmentação das fontes de informação, dificultando a avaliação de sua qualidade por parte do público e contribuindo para o fortalecimento das "câmaras de eco", que serão mencionadas mais adiante;

d. ao mesmo tempo, essas múltiplas e fragmentadas fontes de conteúdo informacional estão concentradas num número restrito de plataformas com números gigantescos de usuários, com algumas empresas controlando várias delas, o que lhes permite acumular enormes quantidades de dados que facilitam a publicidade, mas cujos bancos de dados podem ser indevidamente acessados e manipulados;

e. a existência de "câmaras de eco", ou seja, a tendência de que as pessoas configurem suas

[18] Fica em aberto a questão de se "manipulação social não hostil" seria algo tolerável ou mesmo bem-vindo, na perspectiva dos autores; em alguns momentos, porém, é difícil evitar a impressão de que sim.

[19] Também ficam em aberto: quais seriam esses efeitos nocivos; e para quem eles seriam nocivos.

[20] Na verdade, apesar de fortes discordâncias com importantes aspectos do texto que não poderão ser exploradas aqui, o fato é que a síntese feita em Mazarr et al. (2019) é extraordinária. Tenho acompanhado vários temas que têm pontos em comum com essa discussão há algum tempo, inclusive em sala de aula, e lamento só ter-me deparado com esse texto na elaboração deste trabalho.

plataformas para, consciente ou inconscientemente, acessarem, ainda que de maneira não deliberada, apenas informações que reforcem suas crenças preexistentes; alternativamente, os próprios motores de recomendação das plataformas tendem a proceder desse modo, o que não só mantém as pessoas engajadas na plataforma, como facilita a veiculação de publicidade – o que, paradoxalmente, pode criar nas pessoas a ilusão de que estão acessando múltiplas e diversas fontes e, portanto, de que estariam protegendo-se da tendência de autorreforço de posições prévias;

f. o papel dos influenciadores, isto é, o fato de que algumas pessoas ou pequenos grupos tenham legiões de seguidores, fazendo com que os conteúdos produzidos por esses influenciadores respondam por uma parcela significativa de toda a informação que circula nas plataformas;

g. o fenômeno da trolagem (*trolling*): a produção de informação deliberadamente falsa com o propósito de perturbar a dinâmica normal de comunicação, causar algum tipo de dano, criar constrangimentos ou, simplesmente, em termos mais informais, “por mais lenha na fogueira” para intensificar discussões e inflar as estatísticas sobre a popularidade de determinado assunto ou tema; e

h. por fim, o papel central desempenhado pelos grandes volumes de dados nesse ambiente, o que faz com que cada um desses gigantescos bancos de dados, se acessados indevidamente ou roubados, podem viabilizar campanhas maciças de manipulação informacional (MAZARR et al., 2019, p. 18-40).

Por outro lado, há alguma evidência, ainda que controversa, de que tentativas de confrontar diretamente determinadas informações em que as convicções das pessoas se baseiam não só não funcionariam, como muitas vezes, são contraproducentes (MAZARR et al., 2019, p. 55-57).

Essas características do atual ambiente informacional parecem sugerir o seguinte: é muito difícil que tentativas de manipulação (ou persuasão, ou influência) voltadas para alterar percepções, crenças, atitudes e comportamentos tenham sucesso; é muito mais fácil obter sucesso na tentativa de reforçar posições que as pessoas, grupos e, principalmente, membros de câmaras de eco já adotam. Ainda assim, segundo os mesmos autores, há algumas condições que fazem com que as chances de que a exposição a informações produza mudanças mais substanciais nas pessoas e grupos sejam maiores :

a. quando a informação é bastante repetida, a ponto de tornar-se familiar e amplamente acessível – muitas vezes, até mesmo quando a informação é repetida múltiplas vezes pela mesma pessoa ou fonte[21]: isso porque mensagens familiares tendem a ser menos escrutinadas que as estranhas;

b. quando a informação chega a partir de múltiplas fontes – ainda que, eventualmente, sem o conhecimento de quem as recebe, todas elas estejam reproduzindo o que proveio originalmente de uma única fonte: nesse caso, tende-se a presumir que a informação em questão está baseada em múltiplas e diferentes perspectivas, merecendo, por isso, maior consideração[22];

c. quando outras pessoas do mesmo círculo social (ou da mesma câmara de eco) manifestam receptividade a uma mensagem ou informação: esse é um fenômeno bastante poderoso, o efeito da prova social (*social proof effect*), que se apoia no conformismo, que seria a tendência das pessoas de se adequarem aos comportamentos predominantes nos seus grupos - esse fenômeno, aliás, desempenha importante papel na viralização de mensagens;

[21] Essa ideia remete à fórmula geralmente atribuída a Joseph Goebbels: “*Uma mentira repetida inúmeras vezes torna-se verdade*”.

[22] Em conjunto com o anterior, esse fenômeno incentiva a criação e o funcionamento de robôs para a repetição e a veiculação de mensagens.

d. quando a informação vindoura se encaixa nas crenças e visões de mundo preexistentes do indivíduo: nesse caso, a resistência a uma informação nova ou que contradiga uma outra até então adotada tende a ser bem menor - parece haver processos fisiológicos significativos que favorecem a informação que confirma visões preexistentes;

e. quando a informação faz parte de um relato coerente e amplo, que, por inseri-la num quadro coerente, torna-a mais persuasiva;

f. quando o indivíduo não se sente ameaçado: quanto mais tranquila uma pessoa estiver, mais ela tende a ser receptiva a uma informação;

g. quando o indivíduo confia na fonte da informação, e esta lhe parece crível: informações que pareçam muito estapafúrdias tenderão a ser rejeitadas até mesmo quando se considera confiável a fonte; e

h. curiosamente, por fim, informações negativas tendem a ser mais persuasivas e aceitas por mais tempo, bem como informação que é apresentada em linguagem negativa (MAZARR et al., 2019, p. 48-55).

Cabe aqui uma ressalva: na verdade, as condições acima são as que favorecem a receptividade a uma informação, e não necessariamente a uma informação nova ou conflitante com crenças prévias. Vários desses pontos já haviam sido identificados no magistral estudo de Schudson (1993 [1984]) sobre a indústria da publicidade (e, em menor medida, de relações públicas), basicamente na mesma direção. Ainda assim, elas ajudam a identificar condições em que a manipulação agressiva da informação poderia ser realizada por atores hostis.

No entendimento dos autores, portanto, no atual ambiente informacional ou infosfera, várias técnicas podem ser empregadas, combinadas ou isoladamente, como parte do "guerrear societal virtual":

> Essa forma de guerrear envolve o emprego de agressão largamente não cinética, baseada-em-informação para atacar a estabilidade social de nações rivais. É *virtual* porque, majoritariamente, essas estratégias não empregam violência ou destruição físicas diretas. (Essa concepção, portanto, exclui tanto ataques militares diretos como ataques cibernéticos em larga escala concebidos para produzir caos na infraestrutura física de uma nação e causar dano material.) É *societal* porque tanto os alvos quanto os participantes em tais campanhas estendem-se por toda a sociedade, e porque a meta é solapar o funcionamento efetivo, os níveis de confiança e, ultimamente, a própria estabilidade da sociedade-alvo. E é *guerrear* porque, em suas formas potencialmente mais elaboradas, representam uma atividade concebida para obter supremacia sobre nações rivais, não simplesmente para obter vantagem relativa numa competição continuada, mas sim para obter vitória decisiva de maneiras tais que deixem a nação-alvo sujeita à vontade do atacante. (MORRIS et al., 2019, p. 155, grifos no original).

Essa caracterização do guerrear societal virtual a aproxima bastante da discussão da "zona cinzenta".

3.2 A "zona cinzenta entre paz e guerra"

Embora, no contexto que nos interessa aqui, a expressão "zona cinzenta" (*gray zone*) tenha sido empregada algumas vezes antes (todas em 2015), o primeiro tratamento mais sistemático, até onde nos tenha sido possível identificar, foi feito em Mazarr (2015). Ali, o problema é colocado da seguinte forma:

> Por não quererem arriscar uma escalada de maior porte a partir de aventureirismos militares pura e simplesmente, [Estados insatisfeitos com o *status quo* e determinados a alterar, em seu favor, importantes aspectos da distribuição global de poder e influência] estão empregando sequências de passos graduais para assegurarem-se vantagens estratégicas. Os esforços permanecem abaixo dos limiares que engendrariam resposta robusta dos EUA ou internacional, mas ainda assim são vigorosos e deliberados, calculados para obter tração mensurável ao longo do tempo. [...] Trata-se de estratégias de “fatiar o salame”, fortalecidas com um leque emergente de técnicas de uma área cinzenta ou não convencional – de ataques cibernéticos à ambígua terra-de-ninguém entre guerra e paz, refletindo o tipo de campanhas agressivas, persistentes, determinadas, características do guerrear, mas sem o emprego aberto de força militar. (MAZARR, 2015, p. 1-2).

Essas “campanhas de zona cinzenta” estariam sendo empregadas pela China no Mar da China Meridional, pela Rússia no Leste Europeu (embora, nesse último caso, empregando também força militar), pela busca de armamentos nucleares e de influência regional pelo Irã e até as florescentes estratégias diplomáticas e econômicas de potências ascendentes como Brasil, Turquia e Índia. (MAZARR, 2015, p. 2). Em suma, todos esses, e, potencialmente, mais alguns outros, poderiam ser considerados “revisionistas”, ou seja:

> [...] desejam transformar substancialmente, em seu benefício, regras ou normas internacionais relevantes, a estrutura, os procedimentos de operação de organizações internacionais, a balança de poder ou de influência entre Estados, ou a distribuição de bens internacionais. Revisionistas veem regras, instituições, normas e balanças de poder existentes como insuficientes para atingir seus objetivos, ou injustas, ou enviesadas contra ele, ou alguma combinação de tudo acima. (MAZARR, 2015, p. 14).

Num trabalho posterior, que contou com a participação do próprio Michael J. Mazarr, Morris et al. (2015) enunciam uma definição de “zona cinzenta” que inclui a atividade de atores não estatais:

> A zona cinzenta é um espaço operacional entre a paz e a guerra, envolvendo ações coercitivas para mudar o *status quo* que estão abaixo de um limiar que, na maioria dos casos, suscitaria uma resposta militar convencional, frequentemente embaçando (*blurring*) a linha entre ações militares e não militares e a identificação de autoria (*attribution*) de acontecimentos. (p. 8).

Portanto, as campanhas na “zona cinzenta” seriam para fins revisionistas; permaneceriam aquém de limites reconhecidos para dar início a respostas envolvendo o emprego de forças armadas; desenrolar-se-iam ao longo do tempo, em passos graduais, e não de maneira abrupta ou que cause espécie; e cuja autoria seria frequentemente difícil de estabelecer. Além disso, os autores acrescentam outros aspectos comuns das atividades na “zona cinzenta”:

a. o recurso a “justificativas legais e políticas, frequentemente fundamentadas em reivindicações históricas, com documentação”;

b. ainda para evitar respostas decisivas, campanhas na “zona cinzenta” evitam ameaçar interesses vitais ou existenciais dos seus alvos;

c. por meio do emprego frequente de situações de *faits accomplis*, tais campanhas empregam o risco da escalada do conflito (transferido para o adversário pela ação anterior) como uma fonte de vantagem coercitiva;

d. como parte da abordagem geral de permanecer aquém do limiar da resposta armada,

campanhas na "zona cinzenta" tipicamente seriam baseadas em instrumentos não militares; e

e. por fim, tais campanhas visariam vulnerabilidades específicas nos países alvos. (MORRIS, 2019, p. 8-11).

Ou seja, as campanhas na "zona cinzenta" visariam a "tirar vantagem de ambiguidades estratégicas para obter ganhos graduais" (MORRIS, 2019, p. 12). Nessa perspectiva, então, os EUA já estariam enfrentando competição global na "zona cinzenta" por parte de diversos atores, estatais e não estatais. Uma consequência da existência de "campanhas na zona cinzenta" seria então:

> a perda de nitidez [*blurring*] da linha divisória entre paz e guerra, ou entre empreendimentos [*endeavors*] civis e militares. Elas são, em certo sentido, um emprego de instrumentos civis para alcançar objetivos reservados, algumas vezes, para capacidades militares. Elas colocam toda a sociedade em risco e criam um senso de conflito continuado, mesmo que sem o desdobramento de formações militares tradicionais para tomar território. Campanhas de zona cinzenta, portanto, continuam a tendência de várias formas de conflito – terrorismo, insurgência e ameaças nucleares incluídos – de tornar populações civis um alvo regular. (MAZARR, 2015, p. 62).

Nos termos de Morris et al.:

> A mentalidade tradicional nos EUA, em que "ou estamos em paz ou em guerra" é insuficiente para lidar com essa dinâmica, porque a situação que está emergindo é primariamente "uma competição antagonística com uma dimensão militar sem o conflito armado" (2019, p. 2).

A convergência entre as ideias de "campanhas da zona cinzenta", de guerrear híbrido e de guerrear informacional com ênfase em resultados cognitivos é muito conspícua, e, de fato, vem sendo incorporada doutrinariamente, inclusive na OTAN, como se verá mais abaixo. Entretanto, ela apresenta muitos problemas, particularmente, decorrentes da ideia de "zona cinzenta" e do "guerrear societal virtual". Com efeito, dada a ideia de "revisionismo" que transparece na discussão, qual Estado não seria revisionista? A julgar pela caracterização, somente aqueles que estivessem totalmente satisfeitos com sua posição atual, que se julgassem plenamente atendidos em todos os seus interesses pelas características do sistema internacional e de seus processos de governança, que fossem plenamente satisfeitos econômica e socialmente e que nunca tivessem nada a ganhar. Ainda assim, todos eles teriam a tendência de procurar obter algum tipo de vantagem como *hedging* para o caso de a situação se alterar em seu desfavor.

Reiterando: qual Estado não seria revisionista? Somente aqueles que fossem tão fracos e despossuídos a ponto de temerem qualquer reação a qualquer reivindicação. E, no entanto, Mazarr (2015, p. 15) sugere exatamente o contrário: que, à medida em que os Estados fossem melhorando sua posição, tenderiam a ser menos revisionistas, pois seriam beneficiados pela ordem que lhes permitiu ascender, em primeiro lugar. Esse comentário é surpreendente: e se um dos motivadores da busca por melhoria de posição e de obtenção de vantagens e ganhos estivesse voltada exatamente para permitir-lhe as condições de forçar transformações substantivas nessa ordem? Se o raciocínio acima fosse minimamente válido, então, aí é que não haveria o que temer por parte dos Estados poderosos, e sugeriria até mesmo que distribuir poder – ou fortalecer, voluntariamente, os atores revisionistas – seria uma maneira de preservar a ordem internacional. Então "as democracias", como mencionadas recorrentemente nos textos acima, só teriam a temer os Estados menos poderosos? Esses é que poderiam desestabilizar a ordem global com seu "guerrear societal virtual"? A ideia toda parece não fazer sentido.

Em segundo lugar, toda a ideia de "zona cinzenta entre a guerra e a paz" parece difícil de

sustentar, mesmo nos termos dos proponentes. Como conciliar a ideia, citada acima, de que “campanhas de zona cinzenta, portanto, continuam a tendência de várias formas de conflito – terrorismo, insurgência e ameaças nucleares incluídos – de tornar populações civis um alvo regular” com a ideia de que a “ação na zona cinzenta” fica aquém do limiar de uma resposta armada robusta? Terrorismo e insurgência regularmente engendram respostas armadas e robustas; e, se é para ficar só na ameaça, qual a diferença qualitativa entre ameaças nucleares e ameaças convencionais – pelo menos diante de adversários mais fracos e não nuclearmente armados? Sob esse aspecto, a mera existência de forças armadas poderia ser considerada uma ameaça: ou seja, os EUA já estariam em “guerra informacional” com o mundo inteiro há muito tempo, e, como eles, todos os demais Estados?

Por outro lado, qual tipo de tentativa de melhorar sua própria posição, de usar os trunfos de que se disponha, de usar uma diplomacia agressiva e de tentar obter apoio junto a segmentos da opinião pública de outros países não seria um “guerrear informacional”, uma “campanha na zona cinzenta”? Na verdade, quem parece obscurecer a linha divisória entre guerra e paz são os próprios proponentes da ideia de “zona cinzenta”. Com efeito: “Se a zona cinzenta é definida simplesmente como competição, a diferença entre ela e a condução regular da política internacional não fica clara” (LIBISELLER; MILEVSKI, 2021, p. 104). Faz sentido considerar que o exercício de uma diplomacia mais assertiva por parte, digamos, do Brasil, o colocaria numa situação de hostilidade para com os EUA? Os EUA agiriam com relação ao Brasil nesses termos?

Por fim, parece que os autores não se preocupam tanto com as consequências dessa mistura conceitual. Para além de conceitualmente descabida – pois o que define a guerra é ser uma ação de força –, o enfraquecimento da distinção põe em xeque dispositivos e constrangimentos éticos e jurídicos que protegem exatamente os valores democráticos e a “ordem internacional baseada em regras” que se quereria, supostamente, proteger, como apontado por Echeverría (2015). Os revisionistas que subvertem a ordem internacional baseada em regras são, exatamente, os proponentes da ideia de “zona cinzenta”. É difícil acompanhar essas ideias sem lembrar de outras ocasiões em que, em nome de proteger a democracia, liberdades fundamentais foram suprimidas, não só em outros países (com e sem o apoio dos EUA), mas também nos próprios EUA, como no caso, por exemplo, das perseguições do McCarthyismo. Não por acaso, ao discutir maneiras de enfrentar o desafio do guerrear societal virtual, Morris et al. (2019, p. 163) põem em tela a discussão sobre “a natureza e os limites da liberdade de expressão (*free speech*)”, não sem alertar que “[o] desafio supremo é distinguir entre discurso legítimo e ‘ilegítimo’” (tradução livre). Infelizmente, as aspas não mascaram o fato de que os autores efetivamente se dispõem a discutir restrições ao que pode ser dito, em nome do combate à desinformação – o que, necessariamente, exigiria que alguém tivesse a autoridade para defini-los. É difícil escapar à impressão de que há, no mínimo, uma consideração da possibilidade de que algo equivalente ao “Ministério da Verdade” das distopias políticas venha a materializar-se. Sintomaticamente, essa sugestão parece um claro retrocesso quando comparada à “Linha de Esforço de Informes” do FM 3-13/2013.

4 “ZONA CINZENTA” E “GUERREAR INFORMACIONAL” NA DOUTRINA DA OTAN

As ideias de guerrear informacional e de ambiente internacional não se restringem à literatura acadêmica, mas vêm sendo incorporadas doutrinariamente, e com amplo alcance. Fazem parte, por exemplo, da *Allied Joint Publication 10-1 – Allied Joint Doctrine for Information Operations*.

De acordo com a OTAN, o ambiente informacional é o ambiente "constituído pela própria informação; pelos indivíduos, organizações e sistemas que recebem, processam e transmitem informações; e pelo espaço cognitivo, virtual e físico no qual tudo isso ocorre." (NATO, 2023, p. 15 tradução livre). Esse ambiente seria segmentado em três dimensões, cada uma com suas camadas:

a. a dimensão cognitiva, ou seja, aquela em que os efeitos cognitivos das atividades afetam o pensamento dos indivíduos, de onde decorrem decisões e comportamentos, tem duas camadas:

- camada cognitiva, em que a informação é interpretada pelos indivíduos, mas não é transmitida;

- camada social, em que os comportamentos dos indivíduos são influenciados pelas pressões do ambiente sociocultural sobre as decisões individuais;

b. a dimensão virtual é o espaço virtual em que as audiências interagem virtualmente:

- a camada das ciberpersonas compreende as maneiras como as personas das audiências – inclusive influenciadores, bots e inteligência artificial – manifestam-se e interagem pelos seus perfis online, tanto publicamente, como em mídias sociais, ou mais privadamente, como pelos aplicativos de mensagens; e

- a camada lógica compreende atividades de armazenamento, processamento e transmissão de dados e informações analógicas e digitais; e

c. a dimensão física é constituída pelas áreas geográficas, incluindo os equipamentos e infraestruturas, em que as audiências vivem:

- a camada física de rede é a infraestrutura subjacente às camadas virtuais, e é nela que ocorrem a transmissão e a recepção das informações e dados entre dispositivos e o meio físico da transmissão;

- a camada física é aquela em que as audiências interagem fisicamente e em que existem as infraestruturas humana e técnica de comunicação; e

- a camada geográfica explora a maneira como as audiências habitam a terra (NATO, 2023, p. 37-42).

Ainda de acordo com a AJP 10-1, a dimensão cognitiva seria a mais importante de todas, exatamente por sua importância para a tomada de decisão dos indivíduos.

Consoante com esse entendimento e com a avaliação de que, na "Era da Informação", "a tecnologia" permitiria "enviar, em tempo real, comunicação segmentada por audiências (*audience-tailored communication*), de modo a relatar; transmitir ordens; informar; influenciar; persuadir; confundir; coagir; ou enganar" (NATO, 2023, § 1.3), a publicação manifesta uma insistência quase obsessiva em "controlar a narrativa", diante da firme convicção, também expressa insistentemente ao longo do documento, de que atores hostis explorariam intensamente as atividades de informação de modo a "semear a desconfiança e, potencialmente, exacerbar a agitação (*turmoil*) em diferentes audiências" (NATO, 2023, § 1.4).

Uma preocupação bastante recorrente no documento é a possibilidade de que tais operações de informação sejam conduzidas antes ou sem que haja o emprego da força física, de ações violentas, ou de Forças Armadas, limitando, com isso, a capacidade de resposta de Estados democráticos, com maiores restrições legais em tempos de paz. Desse modo, afirma-se, no documento, que distinções mais nítidas entre guerra e paz já não seriam atuais, devendo-se falar num "*continuum* de competição" cooperação-rivalidade-confrontação-conflito armado, com fronteiras pouco distinguíveis; a região que iria desde uma rivalidade mais intensa até o limiar do conflito armado constituiria uma "zona cinzenta".

Tudo isso, lembre-se, refere-se à discussão da ênfase dada à "dimensão cognitiva" do ambiente informacional, que, de fato, é o aspecto que predomina nos já referidos AJP 10-1, e Declaração da Cúpula no País de Gales, da OTAN, e ainda no *Joint Framework on Countering Hybrid Threats: a European Union Response*, onde se lê:

> Embora as definições de ameaças híbridas variem e precisem permanecer flexíveis para responder à sua natureza em evolução, o conceito visa capturar a mistura de atividades coercitivas e subversivas, métodos convencionais e não convencionais (ou seja, diplomáticos, militares, econômicos, tecnológicos), que podem ser usados de forma coordenada, por atores estatais ou não estatais, para atingir objetivos específicos, permanecendo abaixo do limiar da guerra formalmente declarada. Geralmente, há uma ênfase na exploração das vulnerabilidades do alvo e na criação de ambiguidade para dificultar os processos de tomada de decisão. Campanhas maciças de desinformação, usando as mídias sociais para controlar a narrativa política ou para radicalizar, recrutar e direcionar agentes por procuração podem ser veículos para ameaças híbridas. (EUROPEAN COMMISSION, 2016, tradução livre).

Entretanto, tal entendimento amplo, associado a essa literatura, padece de alguns sérios problemas. Na maioria dos casos, as propostas sobre controle "da narrativa" sugerem uma perspectiva bastante ingênua sobre os processos de propagação de ideias na Internet, e particularmente nas mídias sociais[23]. Com poucas exceções, a literatura parece ignorar o quanto essa propagação depende: (i) dos procedimentos embutidos nos algoritmos de recomendação em geral (por exemplo, dos motores de busca, como Google, Bing ou Duck-Duck-Go), de aplicativos mais específicos (como *streaming* de vídeos e/ou música, ou domínios de compra) e, principalmente, das mídias sociais (a respeito, cf. O'NEIL, 2020; SUMTER, 2019); e (ii) de dinâmicas propriamente sociais, como "bolhas epistêmicas", "câmaras de eco", "guerras de trincheiras" e outros fenômenos (cf. CINELLI et al., 2021; KARLSEN et al., 2021; NGUYEN, 2018; REN et al., 2021) – digamos que falta uma consciência mais clara do forte interrelacionamento entre aquilo a que se refere por "dimensão cognitiva" e as ditas duas camadas da chamada "dimensão virtual" do ambiente informacional. Também preocupantemente, parece que, pelo menos em parte substancial da literatura, falta clareza sobre a extensão em que o "controle da narrativa" por parte das autoridades russas depende de uma capacidade significativa de cerceamento do discurso – incluindo o cerceamento de acesso a mídias como Facebook e o controle governamental das mídias sociais a que a população russa tem acesso, como *Odnoklassniki* e *VKontakte*, ou ainda o *Telegram* (Alyukov et al., 2023).

Em função disso e de outros problemas semelhantes, alguns autores (cf. ECHEVARRÍA, 2015; LIBISERRI; MULIEVSKI, 2021) criticam o enfraquecimento da distinção entre comportamentos e atitudes aceitáveis na ausência de "conflito armado", pois isso poderia implicar risco a alguns dos valores mais caros às sociedades democráticas e ao arcabouço legal que, ironicamente, sustentaria a própria RBIO que se diz querer defender[24].

Como se pode ver, a AJP 10-1 incorpora plenamente muitas das ideias expostas anteriormente, talvez sem, nem mesmo, o grau de sofisticação demonstrado por parte da literatura. Não obstante, algumas das ideias mais problemáticas foram plenamente incorporadas.

[23] Aliás, em que pese sua popularidade, o próprio conceito de "narrativa", tal como parece ser entendido aqui – e principalmente a ideia de "a narrativa" – também mereceria uma discussão mais rigorosa.

[24] De certo modo, aliás, esse aspecto da literatura não deixa de trazer à mente memórias de circunstâncias passadas, em que

4 CONSIDERAÇÕES FINAIS

A ideia que subjaz ao presente texto não é a de apresentar considerações mais incisivas, mas simplesmente de organizar de algum modo alguns conceitos e suas trajetórias, à luz das mudanças nos processos sociais de produção, armazenamento, processamento, circulação e apreensão de informações, e de criar condições que facilitem pesquisas futuras. Procurou-se fazer um mapeamento preliminar da trajetória de discussões sobre "guerra informacional" e "guerrear informacional" no contexto do atual ambiente informacional, tais como apresentados pela literatura. Reitera-se que a utilização dos termos não significa nenhum tipo de endosso. Embora documentos doutrinários e a literatura que os embasa direta ou indiretamente apresentem sugestões interessantes para reflexão e aprofundamento, nem tudo é consistente com vertentes mais sofisticadas da discussão, enquanto outras parecem ter o potencial de conflitar fortemente com valores democráticos. Além disso, ideias como a da "zona cinzenta" parecem pôr em xeque a própria ordem internacional baseada em regras que se pretende proteger. Por fim, várias delas parecem conceitualmente frágeis e inconsistentes, demandando mais reflexão.

Esses resultados sugerem fortemente que tais conceitos precisam ser examinados bem mais a fundo, e discutidos mais sistematicamente, antes de considerar sua incorporação doutrinária pelo Exército Brasileiro. Especialmente, o conceito de "zona cinzenta entre paz e guerra" e a proliferação de expressões que enfraquecem a distinção entre uma e outra tendem a gerar resistências, pois, ainda que não intencionalmente, parecem implicar a adoção mais frequente de procedimentos que sociedades democráticas relutam a tolerar, até mesmo, muitas vezes, em tempos de guerra. Ainda que preliminar, a discussão feita aqui aponta para a pertinência de que a reflexão doutrinária sobre as atividades voltadas para ampliar o apoio (e neutralizar ou enfraquecer resistências) às atividades bélicas que forem legitimamente conduzidas em nome da sociedade brasileira seja uma reflexão com alto teor de originalidade, reforçando os valores que a sociedade brasileira não está disposta a sacrificar – ainda que outros Estados estejam. Existe capacidade intelectual disponível tanto no Exército Brasileiro (e nas demais Forças Singulares) quanto na sociedade brasileira para fazê-lo. Sim, é bom que doutrinas sejam compatíveis com as de aliados; mas não a preço de sacrificar valores que nos são caros.

a preocupação com a "subversão" e a "agitação" supostamente insufladas por potências estrangeiras permitiu, em segmentos expressivos da sociedade, um grau elevado de tolerância social à censura e ao cerceamento da livre circulação de ideias.

REFERÊNCIAS

BLANNIN, P. Modelling information warfare: visualising definitions, fundamental characteristics, and foundational theories of contemporary information warfare. **Journal of Information Warfare**, v. 20, n. 3 (Summer), p. 90-107, 2021.

BLYTE, Wilson; CALHOUN, Luke T. How we win the competition for influence. **Military Review**, May-June, p. 37-47, 2019.

BRASIL. **Glossário das Forças Armadas**. Brasília: Ministério da Defesa, 2015.

CALISKAN, Murat; CRAMERS, P. A. What do you mean by “hybrid warfare”? A content analysis on the media coverage of hybrid warfare concept. **Horizon Insights**, p. 23-35, 2018.

CALISKAN, Murat; LIÉGEOIS, Michel. The concept of ‘hybrid warfare’ undermines NATO’s strategic thinking: insights from interviews with NATO officials, **Small Wars & Insurgencies**, 2020, DOI: 10.1080/09592318.2020.1860374.

CINELLI, Matteo et al. The echo chamber effect in social media. **Proceedings of the National Academia of Sciences**, v. 118, n. 9, 2021.

CLAUSEWITZ, Carl von. **Da Guerra**. São Paulo: Martins Fontes, 1979.

CLAUSEWITZ, Carl von. **On War**. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1989.

CLAUSEWITZ, Carl von. **Vom Kriege**. Berlin: Ullstein, 1999 [1832].

DINIZ, Eugenio. A Austrália, as *Big Techs*, o jornalismo e o debate público. **Synopsis Inteligência Estratégia Diplomacia**. 2021. Disponível em: https://synopsisint.com/a-australia-as-big-techs-o-jornalismo-e-o-debate-publico/. Acesso em: 7 jul. 2023.

ECHEVARRÍA, Antulio. How should we think about ‘Gray-Zone’ Wars? **Infinity Journal**, v. 5, n. 1 (Fall), p. 16-21, 2015.

EUROPEAN COMMISSION. **Joint Communication to the European Parliament and the Council: Joint Framework on countering hybrid threats — a European Union response**. Brussels, 2016.

FABIAN, Sandor. The Russian hybrid warfare — neither Russian nor strategy. **Defense and Security Analysis**, v. 35, n. 3, p. 308-325, 2019.

FIELD MANUAL 100-6. **Information Operations**. Washington, DC: Department of the Army, 1996.

FIELD MANUAL 3-13. **Information Operations: Doctrine, Tactics, Techniques, and Procedures**. Washington, DC: Department of the Army, 2003.

FIELD MANUAL 3-13. **Inform and Influence Activities**. Washington, DC: Department of the Army, 2013.

FIELD MANUAL 3-13. **Information Operations**. Washington, DC: Department of the Army, 2016.

FONTAINE, Richard. **How to defeat hybrid warfare before it starts**. 2019. Disponível em:

defenseone.com/ideas/2019/01/how-defeat-hybrid-warfare-it-starts/154296. Acesso em: 4 jun. 2023.

GALEOTTI, Mark. Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'? **Small Wars & Insurgencies**, v. 27, n. 2, p. 282-301, 2016.

GILLAN, Kevin; PICKERILL, Jenny; WEBSTER, Frank. The information environment of war. **Sociology Compass**, v. 2, n. 6, p. 1833-1847, 2008.

GREIF, Hajo. **Environments of intelligence: from natural information to artificial interaction**. London: Routledge, 2017.

JANIČATOVÁ, Silvie; Mlejnková, Petra. The ambiguity of hybrid warfare: a qualitative content analysis of the United Kingdom's political–military discourse on Russia's hostile activities. **Contemporary Security Policy**, 2021. DOI: 10.1080/13523260.2021.1885921.

KÄIHKÖ, Ilmari. The evolution of hybrid warfare: implications for strategy and the military profession. **Parameters**, v. 51, n. 3, 2021, doi:10.55540/0031-1723.3084.

KARLSEN, Rune et al. Echo chamber and trench warfare dynamics in online debates. **European Journal of Communication**, v. 32, n. 3, p. 257-273, 2017.

KRAMER, Franklin D.; SPERANZA, Lauren M. **Meeting the Russian hybrid challenge: a comprehensive strategic framework**. Brussels: The Atlantic Council, 2017.

LIBICKI, Martin C. The Convergence of Information Warfare. **Strategic Studies Quarterly**, Spring, p. 49-65, 2015.

LIBISELLER, Chiara. "Hybrid warfare" as an academic fashion. **Journal of Strategic Studies**, 2023, DOI: 10.1080/01402390.2023.2177987

LIBISELLER, Chiara; MILEVSKI, Lucas. War and peace: reaffirming the distinction. **Survival**, v. 63, n. 1, February-March, p. 101-111, 2021.

MAROVIC, Jovana. War of ideas: hybrid warfare, political interference, and disinformation. In: VALASEK, Tomas (ed.). **New perspectives on shared security: NATO's next 70 years**. Brussels: Carnegie Endowment for International Peace, 2019.

MAZARR, Michael J. **Mastering the gray zone: understanding a changing era of conflict**. Carlisle, PA: Strategic Studies Institute/ US Army War College Press, 2015.

MAZARR, Michael J.; BAUER, Michael Ryan; CASEY, Abigail; HEINTZ, Sarah Anita; MATTHEWS, Luke J. **The emerging risk of virtual societal warfare: social manipulation in a changing information environment**. Santa Monica, CA: Rand Corporation, 2019.

MOLLANDER, Roger C.; RIDDILE, Andrew; WILSON, Peter A. **Strategic information warfare: a new face of war**. Santa Monica, CA: Rand, 1996.

MORRIS, Lyle J.; MAZARR, Michael J.; HORNUNG, Jeffrey W.; PEZARD, Stephanie; BINNENDJIK, Anika; KEPE, Marta. **Gaining competitive advantage in the gray zone: response options for coercive aggression below the threshold of major war**. Santa Monica, CA: Rand Corporation, 2019.

MUMFORD, Andrew; CARLUCCI, Pascal. Hybrid Warfare: The continuation of ambiguity by other

means. **European Journal of International Security**, n. 8, p. 192–206, 2023.

NGUYEN, C. Thi. Echo chambers and epistemic bubbles. **Episteme**, 2018.

NORTH ATLANTIC TREATY ORGANIZATION. **Allied Joint Publication 10-1: Allied Joint Doctrine for Information Operations**. Bruxelas: NATO Standardization Office (NSO), 2023.

O’NEILL, Cathy. **Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça a democracia**. Santo André, SP: Editora Rua do Sabão, 2020.

PAUL, Christopher. Psychological operations by another name are sweeter. **Small Wars Journal**, 2010. Disponível em: https://smallwarsjournal.com/index.php/blog/psychological-operations-by-another-name-are-sweeter. Acesso em: 7 jul. 2023.

PAUL, Christopher; MATTHEWS, Miriam. The Russian “firehose of falsehoods” propaganda model: why it might work and options to counter it. **Perspectives**, RAND Corporation, 2016.

RÁCZ, András. **Russia’s hybrid war in Ukraine: breaking the enemy’s ability to resist**. Helsinki: The Finnish Institute of International Affairs, 2015.

REN, Zhiying (Bella); DIMANT, Eugen; SCHWEITZER, Maurice. **Social motives for sharing conspiracy theories**. 2021. Disponível em: https://www.researchgate.net/publication/354501829_Social_Motives_for_Sharing_Conspiracy_Theories#fullTextFileContent. Acesso em: 14 nov. 2021.

RENZ, Bettina. Russia and “hybrid warfare”. **Contemporary Politics**, 2016. DOI: 10.1080/13569775.2016.1201316.

RONA, Thomas. **Weapon systems and information war**. Washington, DC: Office of the Secretary of Defense, 1976.

SCHUDSON, Michael. **Advertising, the uneasy persuasion: its dubious impact on American society**. London: Routledge, 2013 [1984].

SCHWILLE, Michael; WELCH, Jonathan; FISHER, Scott; WHITTAKER, Thomas M.; PAUL, Christopher. **Handbook for tactical operations in the information environment**. Santa Monica, CA: Rand Corporation, 2021.

SUMPTER, David. **Dominados pelos números: do Facebook e Google às fake news, os algoritmos que controlam nossas vidas**. Rio de Janeiro: Bertrand Brasil, 2019.

US Army Science Board. **Technical information architecture for command, control, communications, and intelligence**. Washington, DC: Department of the Army, 1996.

US Department of the Army. **FM 100-6: Information Operations**. Washington, DC: 1996.

WITHER, James K. Making sense of hybrid warfare. **Connections**, v. 15, n. 2 (Spring), p. 73-87, 2016.

YU, Susana; WEBB, Gwendolyn. Market adaptation to regulation fair disclosure: the use of industry information to enhance the informational environment. **Journal of Economics and Business**, 89, p. 1–12, 2017.