ESCOLA DE GUERRA NAVAL

CMG (FN) ALEXANDRE HENRIQUE BATISTA BARBOSA

A DESINFORMAÇÃO COMO FERRAMENTA DA GUERRA HÍBRIDA

Rio de Janeiro
2020

CMG (FN) ALEXANDRE HENRIQUE BATISTA BARBOSA

A DESINFORMAÇÃO COMO FERRAMENTA DA GUERRA HÍBRIDA

Tese apresentada como requisito parcial para a conclusão do Curso de Política e Estratégia Marítimas da Escola de Guerra Naval.

Orientador: CF(RM1) Ohara Barbosa Nagashima

Rio de Janeiro
2020

AGRADECIMENTOS

Ao Capitão de Fragata (RM1) Ohara B. Nagashima, pelo envolvimento com o projeto, pelo tempo que dedicou, pelas orientações precisas e por me manter motivado na busca pela excelência.

À minha esposa, Cíntia, e a meus filhos, Bernardo, Maria Eduarda, Victor Hugo e Lucas, pelo amor, pelo apoio incondicional e pela compreensão.

RESUMO

O conflito entre a Rússia e a Ucrânia, em 2014, colocou em evidência o conceito da Guerra Híbrida. Desde a formulação das definições iniciais até os dias de hoje, esse conceito sofreu diversas interpretações e evoluiu, acompanhando as mudanças observadas a cada novo conflito. Diante de toda a repercussão que a Guerra Híbrida tem gerado e da possibilidade de sua aplicação dentro do nosso entorno estratégico, visualizamos a necessidade de aprofundar os conhecimentos sobre o assunto, de modo a embasar a adoção de medidas no campo político e estratégico. O objetivo desta pesquisa é investigar o emprego da desinformação como uma ferramenta da Guerra Híbrida e identificar ações que possam fazer parte de uma estratégia de combate à desinformação dentro desse contexto. Para isso, investigamos o conceito de Guerra Híbrida, suas principais características e instrumentos, em particular a desinformação. Em seguida, descrevemos o modelo de combate à Guerra Híbrida desenvolvido pelo MCDC(CHW) *Project* e traçamos um paralelo com a estratégia adotada, em 2016, pela União Europeia. Em seguida, usando o apoio da estratégia de combate à desinformação adotada pela União Europeia e a estratégia proposta pelo *European Values Center for Security Policy* para combater a desinformação, estabelecemos um conjunto de objetivos e ações que pudessem ser adotados na elaboração de uma estratégia nacional. Por fim, analisamos a eficácia das ações propostas à luz das ações realizadas pelo Rússia em sua campanha de desinformação contra à Ucrânia em 2014. Concluímos que a desinformação se mostrou uma poderosa ferramenta da Guerra Híbrida para moldar a percepção do público interno e externo e controlar a narrativa dos fatos durante o conflito da Rússia contra a Ucrânia em 2014. A pesquisa indicou ainda que os objetivos e ações propostos podem servir como uma base para o desenvolvimento de uma estratégia nacional de combate à desinformação.

Palavras-chave: Guerra Híbrida, Desinformação, Rússia, Ucrânia.

ABSTRACT

The conflict between Russia and Ukraine in 2014 highlighted the Hybrid Warfare concept. From the formulation of the initial definitions to the present day, this concept has undergone several interpretations and has evolved, following the changes observed in every new conflict. In view of all the repercussions that Hybrid Warfare has generated and the possibility of its use within our strategic environment, we feel the need to improve the knowledge on the subject, in order to orient the adoption of measures in the political and strategic levels. The objective of this research is to investigate the use of disinformation as Hybrid Warfare tool and to identify measures that may be part of a strategy to combat disinformation within this context. For this, we investigated the concept of Hybrid Warfare, its main characteristics and instruments, particularly disinformation. Next, we describe the MCDC(CHW) Project countering Hybrid Warfare framework and draw a parallel with the strategy adopted in 2016 by the European Union. Then, using the support of the European Union strategy to counter disinformation and the European Values Center for Security Policy proposed counter-measures, we established a set of goals and measures that could be adopted in the elaboration of a national strategy. Finally, we analyzed the effectiveness of the proposed measures in the light of the actions carried out by Russia in its disinformation campaign against Ukraine in 2014. We conclude that disinformation proved to be a powerful tool of the Hybrid Warfare to shape the perception of the internal and external public and to control the narrative of facts during the Russian conflict against Ukraine in 2014. The research also indicated that the proposed objectives and actions can serve as a basis for the development of a national strategy to counter disinformation.

Key words: Hybrid Warfare, Disinformation, Russia, Ukraine.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

EI - Estado Islâmico
EUA - Estados Unidos da América
FSB - Serviço de Segurança Nacional da Rússia
Hybrid COE - European Centre of Excelence for Countering Hybrid Threats
MB - Marinha do Brasil
MCDC - Multinacional Capability Development Campaign
MCDC(CHW) - Multinacional Capability Development Campaign Countering Hybrid Warfare
MPECI - Militar, Político, Econômico, Civil e Informacional
NBQR - Nuclear, Biológico, Químico e Radiológico
ONG - Organização Não Governamental
OTAN - Organização do Tratado do Atlântico Norte
PMESII - Político, Militar, Econômico, Social, Informacional e de Infraestrutura
UE - União Europeia
USMC - United States Marine Corps

SUMÁRIO

1 INTRODUÇÃO

Com o fim da Guerra Fria, sem o relativo equilíbrio proporcionado pela bipolaridade do poder no mundo, tensões étnicas, religiosas e nacionais, até então suprimidas, afloraram e se manifestaram na forma de diversos conflitos, na sua maioria regionais, como aconteceu nos Balcãs, na Chechênia, no Afeganistão, no Líbano e na Síria. Os aspectos que os diferenciam dos conflitos da época moderna e contemporânea são os atores envolvidos, estatais e não estatais[1], os meios empregados[2], as táticas[3] e as tecnologias[4].

Diversos conceitos e expressões têm sido desenvolvidos para tentar entender e explicar essas novas formas de conflito, empregando desde termos mais tradicionais, como Guerra Não Convencional ou Irregular, até novas denominações como Guerra Assimétrica, Guerra de 4ª Geração, Guerra de Nova Geração (ou Não Linear), Guerra Irrestrita (ou sem limites), Guerra Composta , Conflitos de Zona Cinza e Guerra Híbrida.

O conflito entre a Rússia e a Ucrânia em 2014, com a decorrente anexação da península da Criméia por aquele país, apresentou características semelhantes àquelas que vinham sendo observadas em outros conflitos recentes, como nas guerras no Líbano (2006) e na Georgia (2008) (CHIVVIS, 2017). Para muitos especialistas em defesa, o termo "híbrido" pareceu ser a melhor maneira para descrever a variedade e diversidade de ferramentas e métodos empregados pela Rússia (WITHER, 2016). Hoffman (2007) afirma que esse conceito vinha sendo desenvolvido, desde o início do século, por analistas do Departamento de Defesa dos Estados Unidos da América (EUA) e do *United States Marine Corps* (USMC), que identificaram uma tendência de mistura e embaçamento dos métodos da guerra.

Desde a publicação dos primeiros artigos sobre o assunto, no início do anos 2000, esse conceito foi ganhando repercussão, primeiramente nos Estados Unidos da América e depois na Europa, particularmente após as ações da Rússia na Criméia e no leste da Ucrânia, e o assunto passou a ter grande destaque na política internacional. Além do mundo acadêmico, o assunto já vem sendo abordado nos documentos estratégicos dos EUA e da Europa[5], onde entrou nas pautas de discussão da União Europeia (UE) e da Organização do Tratado do Atlântico Norte (OTAN).

---

[1] Grupos guerrilheiros e terroristas, redes criminosas ou empresas privadas, entre outros.
[2] Como a combinação de sofisticados sistemas de armas junto com o emprego inovador do sistemas antigos, ataques cibernéticos, propaganda online.
[3] Convencionais e irregulares combinadas de forma sinérgica.
[4] Comunicações satelitais, internet, redes sociais, bots, drones, entre outras.
[5] Como a *Quadriennial Defence Review* (EUA, 2010), a *National Military Strategy* (EUA, 2015) e a *National Security Strategy and Strategic Defense and Security Review* (REINO UNIDO, 2015).

Em 2016, a UE criou, com o aval da OTAN, o *European Centre of Excelence for Countering Hybrid Threats* (Hybrid CoE)[6], que tem como propósito auxiliar os Estados e instituições participantes a entender e a se defender de ameaças híbridas. Além disso, a OTAN desenvolve o *Multinacional Capability Development Campaign Countering Hybrid Warfare (MCDC(CHW) Project*[7], um projeto multinacional para ajudar a entender a natureza e o caráter das ameaças híbridas modernas e a se contrapor à guerra híbrida. Dentro desse contexto, de não somente procurar entender o conceito de Guerra Híbrida, mas também de desenvolver medidas para se contrapor a uma ameaça híbrida, tanto a OTAN quanto a UE estão desenvolvendo estratégias para fortalecer suas capacidades defensivas e prevenir ataques híbridos.

Pode parecer que os riscos da Guerra Híbrida estejam limitados às ações da Rússia no teatro europeu. Contudo, estudos recentes já analisam a estratégia de expansão chinesa nos Oceanos Pacífico e Índico à luz do conceito de Guerra Híbrida. Além disso, tanto a Rússia quanto a China têm demonstrado interesse e exercido influência na América do Sul e na África. Segundo Alessandro Paiva de Pinho, a América do Sul reúne ambiente consideravelmente favorável aos conflitos híbridos, devido às condições políticas, econômicas e sociais da região.

Diante de toda a repercussão que o conceito de Guerra Híbrida tem gerado e da possibilidade de sua aplicação dentro do nosso entorno estratégico, visualizamos a necessidade de estudarmos o assunto para o estabelecimento de medidas no campo político e estratégico. Dentro dessa perspectiva, a análise de estratégias de combate à Guerra Híbrida existentes ou propostas por outros países e organizações poderá ajudar a orientar esse debate aqui no Brasil, principalmente se for possível identificar as dificuldades que estão sendo encontradas e os resultados que estão sendo obtidos.

Para melhor orientar o escopo desta tese, será necessário limitarmos seu objeto de estudo. A Guerra Híbrida envolve uma vasta gama de meios e atividades, mas um elemento atual e importante dela, como visto nas ações russas na Ucrânia, é o emprego da desinformação. Assim, sustentaremos nesta pesquisa a tese de que a ambiguidade gerada pela campanha de desinformação da Rússia contra a Ucrânia em 2014 contribuiu para retardar e enfraquecer a resposta a suas ações e buscaremos apresentar uma proposta de ações que possam fazer parte de uma estratégia para combater a desinformação dentro do contexto da Guerra Híbrida. Para isso, vamos analisar a possível eficácia dessas ações, tomando como referência as ações da Rússia no referido conflito.

---

[6] Centro de Excelência Europeu para Combater Ameaças Híbridas, tradução nossa.

[7] A Campanha de Desenvolvimento de Capacidades Multinacionais – Projeto de Combate à Guerra Híbrida, tradução do autor, é uma iniciativa da OTAN projetada para avaliar e desenvolver, colaborativamente, conceitos e capacidades para lidar com os desafios associados com conduzir operações conjuntas, multinacionais e de coligação.

Assim, para que alcancemos o propósito supramencionado, o presente trabalho está organizado em seis capítulos. Após esta introdução, no segundo capítulo, iremos investigar e conceituar a Guerra Híbrida e identificar suas principais características e os principais instrumentos empregados nesse tipo de conflito. Em particular, investigaremos como a desinformação pode ser usada, dentro do escopo mais amplo da Guerra de Informação, como um dos instrumentos da Guerra, de modo a construir o arcabouço teórico necessário para a compreensão da dimensão da ameaça híbrida e da natureza e escopo das ações que deverão ser adotadas para combatê-la.

No capítulo seguinte, descreveremos o modelo formulado pelo *MCDC (CHW) Project* para o combate à Guerra Híbrida, de modo a proporcionar um arcabouço teórico que oriente a elaboração de uma estratégia. Para facilitar a compreensão do modelo teórico e associá-lo a medidas concretas, será descrita, também, a estratégia adotada, em 2016, pela UE para combater a Guerra Híbrida.

No quarto capítulo, aderente ao objeto desta pesquisa, descreveremos as ações constantes na estratégia da UE para o combate à desinformação e o conjunto de medidas propostas pelo *European Values Center for Security Policy*[8] para combater a desinformação, de modo a identificarmos uma proposta de medidas que possam ser adotadas pelo Brasil.

No quinto capítulo, analisaremos as medidas propostas no capítulo anterior à luz das ações realizadas pela Rússia em sua campanha de desinformação contra à Ucrânia em 2014. Essa análise buscará identificar se essas medidas conseguiriam minimizar as vulnerabilidades apresentadas pela Ucrânia, que tornaram possíveis parte das agressões russas, ou se conseguiriam atenuar seus efeitos danosos.

Finalizando este trabalho, no sexto capítulo, apresentaremos as conclusões, mas também indicaremos possíveis linhas de pesquisa futuras sobre o tema que não puderam ser aprofundadas, bem como implicações do estudo para a Marinha do Brasil (MB).

Adiante, apresentaremos os principais conceitos sobre a Guerra Híbrida e, em particular, sobre a desinformação.

[8] Centro de Valores Europeus para a Política de Segurança, tradução nossa. Também conhecido como *European Values Think Tank*, é um instituto não governamental de estudos de defesa.

2 O CONCEITO DE GUERRA HÍBRIDA E SUA EVOLUÇÃO

"If you can't explain it simply, you don't understand it well enough."[9] (Albert Eistein).

Desde o início do conflito na Ucrânia, o conceito de Guerra Híbrida se tornou, de certa forma, um chavão, devido a seu uso cada vez mais difundido pela mídia, pela comunidade acadêmica e pela OTAN[10] para descrever as ações e métodos de operação da Rússia na Criméia e no leste do país. A combinação de forças especiais, cuja origem não podia ser confirmada, milícias locais, pressão econômica, desinformação e exploração de divisões sociais foi difícil de ser enquadrada nos conceitos de guerra tradicionais e, assim, o conceito de Guerra Híbrida foi o que melhor se ajustou a essa realidade (MONAGHAN, 2019). Expressões como ameaça híbrida, agressão híbrida, conflito híbrido e operações híbridas são termos que têm sido empregados para descrever a integração personalizada e de complexidade sem precedentes da abordagem abrangente da guerra no século XXI (ABBOTT, 2016).

Apesar de não ser um conceito novo, tendo surgido em estudos da virada do século que procuravam entender a evolução da natureza dos conflitos atuais, ainda não há convergência conceitual acerca de sua definição, o que, segundo Leal (2015), demonstra a evolução do tema. Para Wither (2016), a existência de muitas definições para a Guerra Híbrida não chega a ser surpreendente, uma vez que o conceito tem sido delineado de maneiras diferentes, porém relacionadas, e essas definições evoluíram em um período relativamente curto de tempo. Outra possível causa para a dificuldade de definir a Guerra Híbrida decorre do fato do conceito, de acordo com Reichborn-Kjennerud e Cullen (2016), ser deduzido pela análise dos diversos conflitos, dessa forma mudando sua definição e significado de acordo com o objeto estudado.

A ausência de um alinhamento conceitual sobre o tema não impede que seu emprego atinja eficiência e eficácia na conquista dos objetivos definidos. Dessa forma, definir a Guerra Híbrida não deve ser apenas um exercício acadêmico. A maneira como o termo é definido e compreendido pode determinar como os Estados percebem e respondem a ameaças híbridas e como eles irão se contrapor a essas ameaças (WITHER, 2016).

Neste capítulo, vamos investigar e conceituar a Guerra Híbrida e identificar suas principais características e os principais instrumentos empregados nesse tipo de conflito. Em

---

[9] "Se você não consegue explicar algo de maneira simples, você não entende esse algo muito bem", tradução nossa. Citação atribuída a Albert Einstein pelo site brainyquote. Disponível em: <brainyquote.com>.

[10] Conforme declaração do General Philip Breedlove, Comandante Supremo Aliado da OTAN em 2014, disponível em <http://www.stripes.com/news/saceur-allies-must-prepare-for-russia- hybrid-war-1.301464>.

particular, vamos investigar como a desinformação pode ser usada, dentro do escopo mais amplo da Guerra de Informação, como um dos instrumentos da Guerra Híbrida. A conceituação resultante e as características identificadas nas pesquisas apresentadas neste capítulo fornecerão o arcabouço teórico necessário para a compreensão das estratégias de combate à Guerra Híbrida, que serão abordadas nos capítulos 3 e 4, e constituirão a base da comparação que usaremos mais adiante, no capítulo 5, quando confrontaremos a estratégia proposta para o combate à desinformação com as realidades observadas no conflito entre a Rússia e a Ucrânia em 2014.

O capítulo será dividido em seis subcapítulos. No primeiro subcapítulo, abordaremos os primeiros conceitos estabelecidos para a Guerra Híbrida. No segundo, iremos identificar as principais características da Guerra Híbrida conduzida por atores não estatais. No terceiro, iremos analisar as mudanças no conceito decorrentes da campanha híbrida russa contra a Ucrânia em 2014. O quarto subcapítulo trará a análise de um modelo desenvolvido com base nessas características para facilitar a compreensão do conceito. Em seguida, vamos identificar os principais instrumentos que podem ser empregados por um ator em uma campanha Híbrida. Por fim, no sexto subcapítulo abordaremos como a desinformação podem contribuir para o sucesso de uma campanha híbrida. Além disso, o APÊNDICE A apresenta a distinção entre o termo Guerra Híbrida e Ameaça Híbrida que, neste trabalho, são empregados como facetas do mesmo fenômeno.

2.1 Conceitos Iniciais

Neste item, vamos identificar como a análise de mudanças observadas em conflitos contemporâneos levaram ao desenvolvimento do conceito da Guerra Híbrida e quais os aspectos mais relevantes desse tipo de conflito, com base em estudos conduzidos no início deste século.

Em 1998, em sua tese para a *Naval Postgraduate School*, Robert G. Walker fez uma das primeiras definições sobre o conceito de Guerra Híbrida. Segundo ele, na guerra contemporânea, haveria a necessidade de se realizar ações estreitamente coordenadas de operações especiais[11] e convencionais, onde as características de ambos os tipos se faziam presentes. Nesse espaço comum aos dois tipos de ação, surgiria uma forma mista de combater, chamada Guerra Híbrida, conforme ilustrado pela FIG. 1.

[11] Operações conduzidas por forças militares e paramilitares especialmente organizadas, treinadas e equipadas para alcançar objetivos militares, políticos, econômicos ou psicológicos por meios militares não convencionais em áreas hostis, negadas ou politicamente sensíveis. Definição apresentada pelo autor, com base na publicação Joint Pub 1-02, "Department of Defense Dictionary of Military and Associated Terms", 1 Dec 1989.

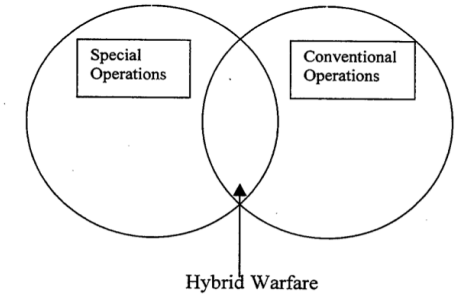

FIGURA 1 – O modelo híbrido de guerra
Fonte: WALKER, 1998, p. 5.

Embora o autor apresente uma definição bem clara do que são operações especiais, ele posteriormente cita as ações norte-americanas durante a Revolução Americana como um exemplo de operações híbridas, pelo emprego combinado de forças regulares e irregulares (as guerrilhas) (WALKER, 1998). Essa comparação tende a confundir o entendimento da definição, uma vez que as guerrilhas que lutavam ao lado de George Washington não podem ser consideradas forças de operações especiais (de acordo com a definição apresentada no trabalho de Walker).

Walker (1998) afirma que, de acordo com os modelos estabelecidos à época para a guerra futura,[12] os conflitos envolveriam cada vez mais o confronto entre forças assimétricas[13] e que a Guerra Híbrida seria o *modus operandi* a ser empregado. Assim, apesar de o emprego convencional de forças continuar a existir, haveria a necessidade de desenvolver forças híbridas, capazes de misturar métodos de emprego convencionais e especiais (ou não convencionais).

Em uma abordagem distinta, William J. Nemeth (2002) realizou uma análise do que ele chamou de sociedades híbridas[14] e suas forças militares. Para ele, a forma dessas sociedades mesclarem táticas irregulares, o emprego inovador de tecnologias modernas e a capacidade de operar fora das convenções do estado de direito e das regras que governam a guerra moderna caracterizariam a Guerra Híbrida (NEMETH, 2012).

Sua tese postula que a Guerra Híbrida representa a versão contemporânea da guerra de guerrilha e dos conflitos assimétricos e que ela se tornaria cada vez mais predominante, sendo a insurgência chechena contra a Rússia, entre 1994 e 1996, um modelo a ser estudado (NEMETH, 2012). Segundo o autor, os chechenos empregaram com sucesso uma fusão de doutrinas militares russas e ocidentais, com táticas de guerrilha descentralizadas e o uso de

[12] O autor cita como referências desses modelos Martin van Creveld, *The Transformation of War*, New York Free Press, 1991; e Alvin e Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*, New York: Warner Books, 1993.

[13] Entre Estados e atores não estatais e entre Estados tecnologicamente e militarmente desenvolvidos contra Estados subdesenvolvidos ou em desenvolvimento (WALKER, 1998).

[14] Sociedades que regrediram para formas mais tradicionais ou primitivas de organização, anteriores a formação dos estados e centradas nos clãs e tribos, mas que levaram consigo os legados da modernidade, como a religião, ideologias políticas, tecnologia e normas sociais. São uma mistura do moderno com o tradicional (NEMETH, 2002).

modernas tecnologias de comunicações para coordená-las em tempo real (NEMETH, 2012).

Essas ideias iniciais contribuíram para estudos que vinham sendo desenvolvidos pelo USMC, que buscavam interpretar características observadas nos conflitos modernos, onde esforços deliberados para embaçar e misturar aspectos da guerra foram identificados (HOFFMAN, 2007). Esses estudos indicavam que forças antagônicas iriam explorar a convergência de diferentes modos de conflito para tentar superar a superioridade tecnológica dos EUA. A partir dessas características, começaram a desenvolver a teoria das ameaças híbridas em uma série de artigos,[15] que culminaram em um estudo produzido por Frank G. Hoffman em 2007, chamado *Conflict in the 21st Century: The Rise of Hybrid Wars*.[16]

Nesse estudo, Hoffman ressalta que o dilema entre preparar suas forças para enfrentar Estados com capacidades convencionais ou atores não estatais empregando táticas assimétricas ou irregulares estaria sendo substituído em função do crescente potencial de envolvimento em conflitos onde a distinção entre guerra e paz e entre combatentes e não combatentes seria cada vez mais difícil. Nesses conflitos, o embaçamento de diferentes modos da guerra, dos atores envolvidos e das tecnologias empregadas ampliariam a variedade e complexidade das ações, no que Hoffman chamou de Guerra Híbrida (HOFFMAN, 2007).

Para Hoffman (2007), o termo "híbrido" refere-se tanto à organização das ameaças híbridas, quanto à forma e aplicação dos meios por ela empregados. Suas forças podem mesclar uma estrutura hierarquizada com o uso de células descentralizadas ou unidades táticas organizadas em rede. Da mesma forma, podem demonstrar modernas capacidades militares enquanto empregam dispositivos explosivos improvisados (HOFFMAN, 2007). O caráter híbrido também é evidenciado pela diversidade dos métodos e táticas empregados e pela natureza difusa das ameaças (HOFFMAN, 2007). Essas combinações dificultam a adaptação e resposta de forças convencionais, treinadas para reagirem de maneira mais linear nas situações de conflito. Segundo o autor,

> Ameaças híbridas incorporam uma vasta gama de diferentes modos de guerra, incluindo capacidades convencionais, táticas e formações irregulares, atos terroristas, incluindo violência indiscriminada e coerção, e desordem criminal. Guerras Híbridas podem ser executadas tanto por atores estatais quanto por uma variedade de atores não estatais. Essas atividades multimodais podem ser executadas por unidades separadas ou mesmo pela mesma unidade, mas são geralmente dirigidas operacional e taticamente e coordenadas dentro do campo de batalha para alcançar efeitos sinérgicos nas dimensões física e psicológica do conflito. (HOFFMAN, 2007, p. 8, tradução nossa.)

[15] MATTIS, James N.; HOFFMAN, Frank G. "Future Warfare: The Rise of Hybrid Wars". Naval Institute Proceedings, Novembro/2005; HOFFMAN, Frank G. "Complex Irregular War: The Next Revolution in Military Affairs.". Orbis, Summer 2006; HOFFMAN, Frank G. "How the Marines are Preparing for Hybrid Wars.". Armed Forces Journal International, abril/2006; HOFFMAN, Frank G. "Preparing for Hybrid Wars.". Marine Corps Gazette, março/2007.

[16] Conflito no Século 21: A Ascenção das Guerras Híbridas, tradução nossa.

Essa definição evidencia dois importantes aspectos do conceito de Guerra Híbrida: seu caráter multimodal e a sinergia de suas ações. Hoffman (2007) considera que os oponentes nos futuros campos de batalha não seguiriam as regras politicamente acordadas para a condução dos conflitos, seja por não se tratarem de atores estatais, seja por operarem abaixo da moldura de uma guerra convencional (embaçamento entre guerra e paz).

Assim, empregariam todos os métodos e ferramentas a seu dispor,[17] combinando a letalidade dos conflitos estatais com o fervor da guerra irregular, de formas inesperadas e cruéis. Fariam uso de tecnologias avançadas de maneiras únicas e não antecipadas, buscando evitar a previsibilidade e obter vantagens, de modo a amplificar os efeitos gerados, tanto na dimensão física quanto na psicológica (HOFFMAN, 2007).

Para ilustrar o conceito, Hoffman (2007) fez uma análise das ações do Hezbollah no confronto com Israel em 2006, no que ele considerou, à época, o exemplo mais claro de um oponente híbrido moderno. Nesse conflito, o Hezbollah, misturando um movimento político organizado com células descentralizadas altamente disciplinadas e bem treinadas,[18] surpreendeu Israel pela combinação de táticas (militares convencionais e de guerrilha) e a aplicação inovadora de tecnologias,[19] em centros urbanos densamente povoados (HOFFMAN, 2007). Outro aspecto não esperado por Israel foi o emprego de armamentos e sistemas de comunicação normalmente associados a Forças Armadas.[20] Além disso, o Hezbollah foi mais eficiente do que Israel em influenciar a opinião pública mundial, empregando a internet e outras mídias (HOFFMAN, 2007).

Hoffman (2007) conclui seu estudo afirmando que o caráter emergente dos conflitos, com o embaçamento das linhas que separam os modos da guerra, não permitiria mais a clara distinção entre forças convencionais e irregulares, combatentes e não combatentes e entre os domínios físico e virtual. Dessa forma, para combater nas Guerras Híbridas, as forças não podem ser projetadas para uma missão única, mas sim para serem multipropósito, flexíveis e possuírem grande capacidade de atuar com outras agências, uma vez que o emprego de todos os instrumentos (ou expressões) do poder nacional será necessário, assim como a integração de

[17] Por exemplo, misturando capacidades de alta tecnologia (como armamentos contra satélites), com terrorismo e ataques cibernéticos direcionados contra o sistema financeiro.

[18] O grau de treinamento, disciplina de fogos e desenvolvimento tecnológico eram muito superiores ao que as tropas israelenses vinham encontrando em suas operações de contraterrorismo na Faixa de Gaza e nos territórios ocupados a oeste (HOFFMAN, 2007).

[19] Em particular, os sistemas de mísseis anticarro empregados pelo Hezbollah contra os blindados israelenses e posições defensivas juntamente com táticas descentralizadas foram considerados surpreendentes oeste (HOFFMAN, 2007).

[20] O Hezbollah fez uso de mísseis de cruzeiro antinavio C802 e rajadas de foguetes. Além disso, há evidencias de que o Hezbollah investiu em inteligência de sinais e monitorou chamadas telefônicas de celular das Forças Armadas de Israel, bem como informes não confirmados de que eles conseguiram decriptografar tráfego de mensagens dos rádios com salto de frequência dos israelenses (HOFFMAN, 2007).

efeitos cinéticos e não cinéticos (HOFFMAN, 2007). Por fim, para o autor, as Guerras Híbridas iriam exigir uma profunda compreensão do contexto histórico e cultural do conflito,[21] dada a necessidade de vencer o duelo de narrativas junto às grandes massas e à opinião pública internacional pela exploração da mídia moderna.[22]

Da análise desses conceitos iniciais, percebe-se que atores não estatais envolvidos nos conflitos contemporâneos apresentaram capacidades superiores àquelas empregadas anteriormente, mesclando táticas irregulares e convencionais com o emprego inovador de tecnologias modernas. Dessa análise, surgiram os conceitos iniciais para a Guerra Híbrida. Para o presente trabalho, consideraremos que o conceito inicial da Guerra Híbrida envolve o emprego não convencional de diversas capacidades, táticas e meios, buscando alcançar efeitos sinérgicos nas dimensões físicas e psicológicas do conflito.

2.2 Características da Guerra Híbrida Conduzida por Atores não Estatais

Com base no conceito apresentado, iremos identificar, a seguir, as principais características da Guerra Híbrida conduzida por atores não estatais. A compreensão dessas características facilitará o entendimento das medidas propostas para o combate à Guerra Híbrida.

De acordo com Reichborn-Kjennerrud e Cullen (2017), esses conceitos iniciais de Guerra Híbrida foram uma tentativa de descrever a crescente sofisticação e complexidade com que atores não estatais vinham conduzindo conflitos como os da Chechênia e do Líbano, no início deste século. Para esses autores, o termo "híbrido" ilustrava a capacidade desses atores não estatais realizarem ações com características da guerra convencional e não convencional, combinadas com modos de operação não militares (terrorismo, extorsão e criminalidade), de maneiras inovadoras que dificultavam sua compreensão pelas forças convencionais (REICHBORN-KJENNERRUD; CULLEN, 2016).

Dentro do contexto apresentado por eles, a Guerra Híbrida conduzida por atores não estatais apresentava duas características marcantes: o elevado nível de sofisticação militar e a expansão do campo de batalha além do domínio meramente militar (REICHBORN-KJENNERRUD; CULLEN, 2016). A primeira característica seria representada pelo emprego de modernos sistemas de armas, tecnologias e táticas consideradas além do alcance de

[21] Para Hoffman (2007), para dominar a dimensão (ou espaço de batalha) da informação, os EUA deveriam centrar seus esforços no fator humano ou cultural, ao invés da ênfase na tecnologia e nas redes de computadores, como eles vinham fazendo no que ele chama de Longa Guerra contra o Extremismo Islâmico.

[22] Que Hoffman (2007) considera ser a mais significativa mudança no caráter do conflito moderno.

adversários não estatais (REICHBORN-KJENNERRUD; CULLEN, 2016). A capacidade de mesclar essa sofisticação com suas habilidades não convencionais dentro do mesmo espaço de batalha seria, segundo os autores, o aspecto novo e característico da Guerra Híbrida não estatal (REICHBORN-KJENNERRUD; CULLEN, 2016).

A segunda característica viria associada à crescente importância de emprego de ferramentas não militares, que confeririam vantagens assimétricas aos atores não estatais em um conflito com atores militarmente superiores (REICHBORN-KJENNERRUD; CULLEN, 2016). Essas ferramentas iriam muito além do uso coordenado do terrorismo e da criminalidade, podendo incluir instrumentos legais para restringir a liberdade de ação do ator estatal e a guerra de informação (no controle da narrativa, mobilização ideológica e recrutamento) (REICHBORN-KJENNERRUD; CULLEN, 2016).

Essa característica fica evidente ao analisarmos a definição de ameaça híbrida empregada por Russell W. Glenn (2009) em um seminário:

> Qualquer adversário que, simultaneamente e adaptativamente, empregue uma combinação qualquer de meios políticos, militares, econômicos, sociais e de informação e métodos de guerra convencionais, irregulares ou catastróficos, terrorismo e atividades disruptivas ou criminais. Pode incluir uma combinação de atores estatais e não estatais. (GLENN, 2009, p. 2, tradução nossa.)

Para Wither (2016), a ênfase em métodos não militares é o principal diferencial da Guerra Híbrida, em particular o emprego de operações de informação coercitivas. Nesse último aspecto, o autor compara a campanha do Estado Islâmico (EI) no Oriente Médio com as operações da Rússia na Ucrânia, dois contextos bem diferentes, mas ambos enquadrados como exemplos de Guerra Híbrida.[23] Nos dois casos, o uso da mídia, especialmente pela internet, foi marcante, porém com objetivos distintos.

O EI buscou glorificar sua causa fazendo uso de mídias sociais e utilizou vídeos de propaganda para recrutar milhares de combatentes estrangeiros (WITHER, 2016). Hoffman (2007) ratifica essa opinião, ao afirmar que a exploração das novas plataformas da mídia pode ser a mudança mais significativa no caráter do conflito moderno por permitir alcançar grandes massas.

Já a Rússia, empregou operações de informação, em particular a desinformação, para influenciar e moldar a percepção pública sobre suas ações, explorando as vulnerabilidades sociais existentes, enfraquecendo as instituições do estado e minando a legitimidade percebida do estado ucraniano (KOFMAN *et al*, 2017). A importância dada às operações de informação

[23] Segundo Wither (2016, p. 76), "o Estado Islâmico efetivamente combinou táticas convencionais e de guerrilha com atos grosseiros de terrorismo, mas também explorou a propaganda e a guerra de informação em um nível sem precedentes para um ator não estatal" , tradução nossa.

na Guerra híbrida seria o reconhecimento de que a opinião pública é um dos centros de gravidade dos conflitos armados contemporâneos.

Considerando os aspectos apresentados, pode-se perceber que a Guerra Híbrida conduzida pelos atores não estatais tem como principais características a capacidade de mesclar uma elevada sofisticação militar com habilidades não convencionais e o emprego eficaz de meios não militares, como a criminalidade, o terrorismo, instrumentos legais, ataques cibernéticos e a desinformação.

2.3 A Guerra Híbrida Conduzida por Estados

Os conceitos estabelecidos inicialmente foram abalados pelas ações da Rússia na Ucrânia em 2014. Veremos neste item como a campanha russa mudou o entendimento que havia sobre a Guerra Híbrida, causando a evolução do conceito.

A anexação da Criméia pela Rússia e a subsequente desestabilização do leste da Ucrânia foram executadas por meio de ações cinéticas de forças especiais em conjunção com uma série de ações diplomáticas, cibernéticas, econômicas, informacionais e psicológicas muito bem planejadas e sincronizadas, no que foi caracterizado como Guerra Híbrida (ABBOTT, 2016). Para muitos especialistas, o termo "híbrido" pareceu ser a melhor maneira para descrever a variedade e diversidade de ferramentas e métodos empregados.[24] Anders Fogh Rasmussen, Secretário-Geral da OTAN no período do conflito, caracterizou as táticas russas como Guerra Híbrida, por envolverem a combinação de ações militares ostensivas e sigilosas e um agressivo programa de desinformação (LANDLER; GORDON, 2014).

Embora as definições de Guerra Híbrida incluíssem seu emprego por atores estatais e não estatais, o conceito foi centrado nos atores não estatais pois foram estes os modelos estudados sobre o conceito (Chechênia e Hezbollah). As ações da Rússia na Ucrânia representaram um desenvolvimento significativo do conceito, pois, diferentemente do que vinha sendo observado, não foi empregado um ator não estatal enfrentando um oponente mais forte, buscando uma vantagem tática e estratégica. Dessa vez, foi um ator estatal, mais poderoso do que seu oponente, que fez uso de ferramentas não militares para reduzir sua exposição ao escrutínio político e jurídico internacional e moldar a narrativa dentro do contexto da guerra de informação/psicológica (ABBOTT, 2016).

[24] As técnicas russas incluíram a tradicional combinação de operações de combate convencionais e irregulares, mas também o apoio e patrocínio a protestos políticos, coerção econômica, operações cibernéticas e, em particular, uma intensa campanha de desinformação (WITHER, 2016).

Diante dessa nova ameaça (ou de uma ameaça renascida), os setores de defesa na Europa passaram a dar mais atenção ao comportamento assertivo da Rússia, o que levou o conceito de Guerra Híbrida a tornar-se um aspecto central nas discussões entre as lideranças civis e militares da OTAN e da UE (HOFFMAN, 2018). Os vários textos sobre Guerra Híbrida passaram a focar em um conjunto similar de atividades que a Rússia empregou na Ucrânia, na Georgia e em outros países vizinhos e que, muitos acreditavam, voltaria a empregar no futuro (RADIN, 2018).

Como exemplo dessa nova interpretação, o *International Institute for Strategic Studies*,[25] na edição de 2015 da revista *Military Balance*, apresentou uma definição bem ampla dessa manifestação mais recente da Guerra Híbrida, focando nos métodos empregados:

> uso de instrumentos militares e não militares em uma campanha integrada, projetada para alcançar surpresa, tomar a iniciativa e obter vantagens psicológicas e físicas empregando meios diplomáticos; rápidas e sofisticadas operações de informação, eletrônicas e cibernéticas; ações militares e de informação secretas e, ocasionalmente, ostensivas; e pressão econômica (THE MILITARY BALANCE, 2015, p. 5, tradução nossa).

Conceitualmente, a Guerra Híbrida conduzida por Estados não é diferente daquela conduzida por atores não estatais. Porém, a capacidade de integração dos meios militares e não militares do poder de um Estado para alcançar seus objetivos políticos potencializa os efeitos sinérgicos gerados, tornando-os multiplicadores de força (REICHBORN-KJENNERRUD; CULLEN, 2016).

Além da amplitude de instrumentos a seu dispor, outra característica da Guerra Híbrida dos Estados, muito utilizada pela Rússia, é o emprego estrategicamente inovador da ambiguidade.[26] Segundo Reichborn-Kjennerrud e Cullen (2017), a ambiguidade é usada na Guerra Híbrida para nublar a intenção por trás das ações do ator envolvido, complicando o processo de tomada de decisão do oponente e dificultando a adoção de uma resposta militar ou mesmo política. Para que isso ocorra, as ações devem ser planejadas para ficar abaixo da percepção do que caracteriza um ato de guerra, de modo a tornar ilegítima (ou pelo menos politicamente irracional) uma resposta militar.

Ainda segundo Reichborn-Kjennerrud e Cullen (2017), a ambiguidade pode ser operacionalizada de várias maneiras: pode-se identificar os limites para resposta[27] estabelecidos pelos oponentes para identificar atos de guerra e operar abaixo desses limites; pode-se encontrar

[25] Instituto Internacional para Estudos Estratégicos, tradução nossa.
[26] Definida por Andrew Mumford e Jack McDonald no relatório *Ambiguous* Warfare como "ações hostis que são difíceis para um Estado identificar, atribuir autoria ou definir publicamente como emprego coercitivo da força", tradução nossa (MUMFORD; MCDONALD, 2014 *apud* REICHBORN-KJENNERRUD; CULLEN, 2016).
[27] Do original *Threshold*, tradução nossa.

zonas cinzas em que esses limites de alerta não tenham sido estabelecidos e explorar essas áreas; ou pode-se enfatizar o emprego de meios não militares, mantendo os meios militares fora das vistas. Outra forma de gerar ambiguidade é por meio da negação plausível,[28] que pode ser alcançada escondendo ou negando o envolvimento do ator estatal pelo emprego de proxies ou de forças cujas origens não possam ser estabelecidas (como os pequenos homens verdes no leste da Ucrânia) ou pela realização de ataques cuja autoria não possa ser atribuída (como em ciberataques), com uma certeza além de qualquer dúvida (REICHBORN-KJENNERRUD; CULLEN, 2016).

Pode-se perceber que a campanha da Rússia na Ucrânia deu uma nova perspectiva ao conceito de Guerra Híbrida. Suas ações passaram a ser a nova referência a ser analisada e explicada e o conceito evoluiu, passando a apresentar novas definições que abrangessem a dimensão mais ampla que o poder estatal trouxe a esse campo de batalha. Essa nova abordagem focava na potencialização dos efeitos alcançados pela maior disponibilidades de meios militares e não militares a serem empregados e na capacidade de coordenação que os Estados possuem. A principal característica identificada era o emprego da ambiguidade, obtida por meio de ações projetadas para evitar os limites para resposta estabelecidos e da negação plausível.

2.4 O Modelo para a Guerra Híbrida

De acordo com Reichborn-Kjennerrud e Cullen (2016), os diferentes entendimentos sobre a Guerra Híbrida centradas em atores estatais e não estatais aumentaram a nebulosidade do conceito. Para torná-lo mais claro, os autores desenvolveram um modelo que será analisado neste item, de modo a facilitar sua compreensão.

O modelo foi desenvolvido incorporando diversas características da Guerra Híbrida estatal e não estatal, e foca nas capacidades e vulnerabilidades dos atores, bem como na forma com que os meios são empregados e nos efeitos desejados (REICHBORN-KJENNERRUD; CULLEN, 2016). Esse modelo foi baseado na seguinte descrição da Guerra Híbrida: “O emprego sincronizado de múltiplos instrumentos do poder adaptados a vulnerabilidades específicas em todo o espectro de funções da sociedade para atingir efeitos sinérgicos.” (Reichborn-Kjennerrud e Cullen, 2017, p. 8, tradução nossa).

De acordo com a definição dada, um ator identifica as vulnerabilidades existentes

[28] Capacidade de negar conhecimento ou responsabilidade por um ato condenável por falta de provas que possam confirmar sua participação.

nas funções críticas[29] de uma sociedade alvo e emprega todos os instrumentos do poder[30] a seu dispor para explorá-las, selecionando aqueles que melhor se adequem à vulnerabilidade encontrada e ao efeito desejado, de modo a alcançar seus objetivos políticos (REICHBORN-KJENNERRUD; CULLEN, 2016). O emprego personalizado dos instrumentos do poder corresponde ao caráter multimodal da Guerra Híbrida e permite que uma ameaça híbrida varie os meios empregados, assim como sua intensidade.

Esse processo pode ser representado graficamente, com os instrumentos do poder distribuídos em um eixo horizontal e a intensidade com que eles são empregados no eixo vertical, conforme a FIG. 2:

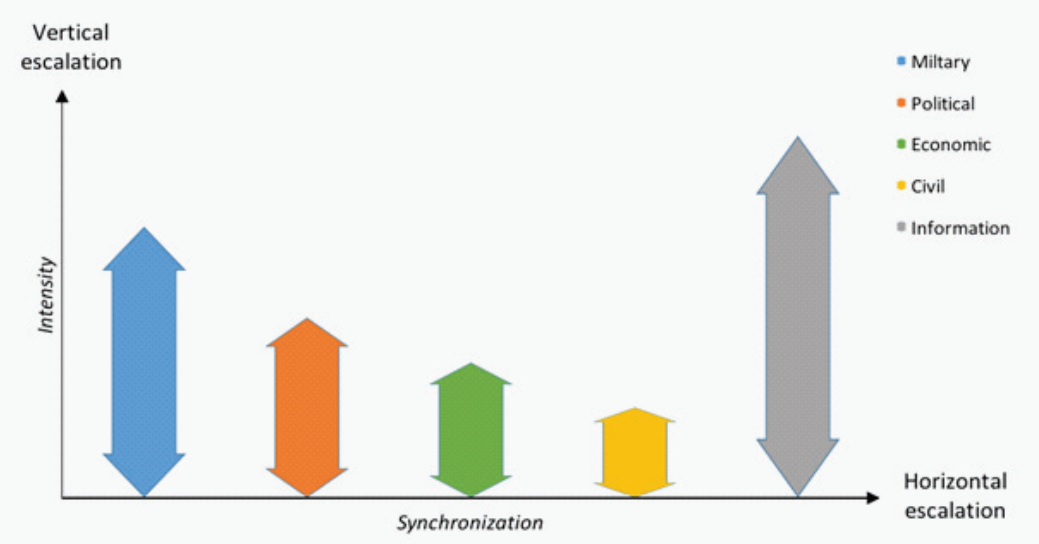

FIGURA 2 – Modelo para escalada horizontal e vertical da Guerra Híbrida
Fonte: REICHBORN-KJENNERRUD; CULLEN, 2016, p. 3.

A variação dos meios empregados e de sua intensidade pode ser vista como uma escalada horizontal (alternando a ação entre os instrumentos do poder) e uma escalada vertical (aumentando ou diminuindo a intensidade utilizada em cada ação), que podem ocorrer simultaneamente (REICHBORN-KJENNERRUD; CULLEN, 2016). Assim, uma ameaça híbrida pode alternar suas ações, escalando ou desescalando a intensidade dos meios empregados, separadamente ou de maneira combinada, para criar efeitos sinérgicos muito superiores aos que cada instrumento isoladamente poderia alcançar (REICHBORN-KJENNERRUD; CULLEN, 2016). Contudo, para que esses efeitos sejam alcançados, é necessário um elevado grau de coordenação e sincronismo, o que requer, por parte do ator

[29] Organizadas nos campos político, militar, econômico, social, informacional e de infraestrutura (PMESII), REICHBORN-KJENNERRUD; CULLEN, 2016.
[30] Organizados nos campos militar, político, econômico, civil e informacional (MPECI), REICHBORN-KJENNERRUD; CULLEN, 2016.

híbrido, uma grande capacidade de coordenação no nível estratégico (para variar os instrumentos do poder e, dentro destes, o meio a ser utilizado) e de centralização do comando e controle no nível operacional (para que a execução ocorra como desejado, principalmente quanto à intensidade da ação) (REICHBORN-KJENNERRUD; CULLEN, 2016).

Essa conjugação de esforços multiplica a força do efeito produzido, permitindo que o mesmo impacto da grande escalada vertical de um meio seja alcançado por uma ação de menor intensidade em outros meios (escalada horizontal), conjugados ou não (REICHBORN-KJENNERRUD; CULLEN, 2016). A manutenção de ações de baixa intensidade nos vários instrumentos do poder contribui, como já citado anteriormente, para a ambiguidade dessas ações, uma vez que ficam abaixo dos limites para resposta estabelecidos pelo oponente, gerando dúvida quanto às suas intenções e dificultando o processo de tomada de decisão para uma resposta, atuando, assim, nos elementos cognitivos da guerra.

Ao atuar de maneira difusa com todos os elementos do poder contra as funções críticas do oponente, o ator híbrido expande o campo de batalha além dos domínios tradicionais (terrestre, marítimo, aéreo, espacial e cibernético), nos espectros político, econômico, psicossocial e informacional. Ao dificultar a compreensão da situação, devido ao caráter ambíguo de suas ações, ele passa a explorar o domínio cognitivo do oponente, em que a batalha nos espaços cognitivo e psicológico para conquistar corações e mentes e controlar a percepção da situação se tornam um aspecto fundamental para a consecução dos objetivos políticos e estratégicos.

Embora esses espaços sempre tenham tido um papel de destaque nas guerras, as características das sociedades modernas, decorrentes do avanço tecnológico alcançado nas últimas décadas,[31] facilitam a execução e o controle das ações em todo o espectro de suas funções críticas (PMESII) e tornam os efeitos dessas ações nos espaços cognitivo e psicológico muito mais eficientes (REICHBORN-KJENNERRUD; CULLEN, 2016). No entendimento deste autor, essa é a principal característica do conceito de Guerra Híbrida.

Dentro desse modelo desenvolvido por Reichborn-Kjennerrud e Cullen (2017), o peso do poder militar é reduzido pela conjugação com outros meios não militares para alcançar os efeitos estratégicos desejados, embora o uso da força ou sua ameaça continue a ter um papel central. Esse conjugado dependerá das capacidades do ator híbrido para identificar as vulnerabilidades do oponente e empregar os instrumentos do poder à sua disposição. Como os atores estatais dispõem de uma gama mais ampla e sofisticada de instrumentos, eles tenderão a

[31] Como a interconectividade; a amplitude, facilidade e velocidade de acesso à informação; digitalização das economias e dos sistemas de controle de infraestrutura; a interdependência das economias (REICHBORN-KJENNERRUD; CULLEN, 2016).

ser mais aptos a realizar essa escalada horizontal e vertical das ações e, consequentemente, mais eficientes na condução na Guerra Híbrida.

Para Reis Friede (2018),[32] somente os atores não estatais mais bem sucedidos e financiados teriam essas capacidades. Além disso, por não coordenarem o emprego de forças regulares e irregulares (por não possuírem as primeiras), as ações desses atores não se enquadrariam na definição de Guerra Híbrida. Essa análise é falha, uma vez que o conceito não define ou restringe os meios a serem empregados, muito menos como eles serão empregados, mas apenas que eles devem buscar efeitos sinérgicos. Além disso, como citado anteriormente, limitações para a escalada horizontal entre instrumentos podem ser compensadas pela escalada vertical dos meios disponíveis.

Com base nos aspectos analisados neste item, percebe-se que o modelo estudado para a Guerra Híbrida é o que melhor representa o seu caráter multimodal. Assim, para o interesse da presente pesquisa, consideraremos a definição de Reichborn-Kjennerrud e Cullen (2017) de que a Guerra Híbrida envolve o emprego sincronizado de múltiplos instrumentos do poder adaptados a vulnerabilidades específicas em todo o espectro de funções da sociedade para atingir efeitos sinérgicos. A seleção dos meios e de sua intensidade pode, então, ser representada graficamente, caracterizando a escalada horizontal e vertical das ações. A conjugação dos esforços pode gerar efeitos multiplicadores de força e contribuir para a ambiguidade. Com isso, a Guerra Híbrida consegue expandir o campo de batalha para os espaços cognitivos e psicológicos, fortalecendo a batalha por corações e mentes.

2.5 Instrumentos Empregados na Guerra Híbrida

Além de compreender o conceito de Guerra Híbrida, para que se possa definir ações para combate-la é necessário saber quais os instrumentos que podem ser empregados dentro do seu contexto. Assim, iremos identificar alguns instrumentos propostos na literatura sobre o tema.

Apesar de Reichborn-Kjennerrud e Cullen (2017) e Abbott (2016) afirmarem ser difícil estabelecer uma lista genérica de instrumentos que possam ser empregados na Guerra Híbrida, por ser uma decisão que depende muito do contexto, Chivvis (2017) relaciona Operações de Informação, Operações Cibernéticas, o emprego de *proxies*, influência

[32] Citando artigo do site Dinâmica Global: "Entendendo a Guerra Híbrida: Uma Análise Explicativa, Traz a Definição de Guerra, Não-Guerra e Tipos de Guerra". Disponível em: < https://dinamicaglobal.wordpress.com/2016/08/31/entendendo-a-guerra-hibrida-uma-analise-explicativa-traz-a-definicao-de-guerra-nao-guerra-paz-e-tipos-de-guerra/>.

econômica, ações clandestinas e influência política como ferramentas de Guerra Híbrida empregadas pela Rússia.

Alinhado com Chivvis, Treverton *et all* (2018) fazem uma análise das ferramentas que, segundo os autores, podem ser empregadas por uma Ameaça Híbrida. O QUADRO 4 (ANEXO A – Variedade de ferramentas híbridas) lista essas ferramentas. Já Monaghan (2017) apresenta uma lista de potenciais instrumentos não violentos que podem ser empregados e de possíveis tipos de guerra que provavelmente serão combinados por um adversário híbrido durante um conflito armado, como pode ser visto nos QUADROS 5 e 6 (ANEXO B – Instrumentos militares e não militares da Guerra Híbrida). Segundo ele, essa lista visa auxiliar a determinar o escopo de estratégias de defesa e para a definição de capacidades no desenvolvimento de forças.

Todos os meios, ferramentas e tipos de guerra citados anteriormente podem ser empregados em um conflito híbrido. Mesmo com a separação entre Ameaça Híbrida e Guerra Híbrida dentro do *Continuum* do Conflito, onde a caracterização da "guerra" se torna mais ou menos evidente, é muito difícil diferenciar o emprego dos meios não militares na fronteira entre essas duas categorias, principalmente quando ocorrem simultaneamente. É difícil, também, estabelecer uma precedência ou identificar qual dessas ferramentas é mais importante ou eficiente.

Porém, para muitos autores, como já citado anteriormente, a exploração das novas plataformas de mídia para a condução da Guerra de Informação em todas as suas formas, aí incluídas a propaganda, a desinformação, o uso de notícias falsas, mídias sociais e meios de comunicação domésticos é um dos aspectos mais marcantes da Guerra Híbrida.[33] Para o General Philip Breedlove,[34] a mais impressionante novidade da Guerra Híbrida na Ucrânia foi o emprego de diferentes ferramentas de informação na criação de uma narrativa falsa (MCCANEY, 2015), no que ele descreveu como a mais fantástica blitzkrieg já vista na história da Guerra da Informação.[35]

Diante do exposto, percebe-se que a evolução dos meios de comunicação tem tornado cada vez mais eficaz o emprego da informação como uma arma. Embora não seja algo novo, a Guerra da Informação vem sendo empregada com maior sofisticação e intensidade. As

[33] "Outra implicação é a necessidade de incorporar o que pode ser a mais significante mudança no caráter do conflito moderno, a exploração da mídia moderna para alcançar grandes massas e mobilizá-los para suportar uma causa" (HOFFMAN 2007, p 51). "O emprego de operações de informação coercitivas é o fator mais distinto das descrições recentes da Guerra Híbrida..." (WITHER, 2016, p 76).

[34] Comandante Supremo Aliado da OTAN em 2014.

[35] John Vandiver, "SACEUR: Allies Must Prepare for 'Hybrid Warfare,'" Stars and Stripes, 4 de setembro 2015. Disponível em: <www.stripes.com/news/saceur-allies-must-prepare-forrussia-hybrid-war-1.301464>.

ações da Rússia na Ucrânia foram um exemplo da contribuição que a Guerra da Informação pode dar dentro da estratégia mais ampla da Guerra Híbrida.

Nesse contexto, a desinformação é uma ferramenta importante para moldar a percepção dos envolvidos. Dessa forma, torna-se necessário entender como o uso da desinformação influência a condução da Guerra Híbrida para podermos formular estratégias para combatê-la, o que faremos a seguir. O APÊNDICE B – A informação como uma arma traz uma base teórica sobre a Guerra da Informação para permitir uma melhor compreensão do contexto amplo em que a desinformação pode ser empregada.

2.6 O Uso da Desinformação na Guerra Híbrida

De acordo com Kelly e Paul (2020), no que se refere à guerra moderna, informação é a nova munição. A transformação da informação em uma arma, chamada de Guerra da Informação, é um elemento chave da Guerra Híbrida. Considerando a relevância da desinformação para a Guerra Híbrida, é importante entender melhor seu conceito, suas características e quais os efeitos que ela pode produzir.

De acordo com Kelly *et al* (2017), há mais de 30 países que vêm empregando diferentes formas de desinformação, inclusive dentro de seus próprios países. Para a Comissão Europeia (2018a), a exposição das sociedades à desinformação em larga escala é o maior desafio para a Europa. Já Lucas e Pomerantsev (2016) afirmam que o uso da desinformação vem crescendo em sofisticação, alcance, intensidade e impacto e que a era da informação está se transformando, rapidamente, na era da desinformação.

A UE define desinformação como "uma informação comprovadamente falsa ou enganosa que é criada, apresentada e disseminada para se obter ganho econômico ou para enganar intencionalmente a população, podendo causar dano público" (COMISSÃO EUROPEIA, 2018b, p. 4, tradução nossa). [36] Ela se diferencia da propaganda basicamente pelos objetivos e pela forma de disseminação. Enquanto a propaganda está associada a táticas e estratégias em apoio a uma causa política, ideologia ou interesse específico e, normalmente, emprega campanhas publicitárias ousadas ou ações de inteligência sigilosas, a desinformação é uma maneira de fomentar a desconfiança e a antipatia a práticas e normas estabelecidas (FIOTT; PARKES, 2019). Ela não é fácil de detectar e não possui uma causa ou mensagem política discernível, podendo, em muitos casos, ser confundida com teorias da conspiração (FIOTT;

[36] Dano público compreende ameaças aos processos políticos democráticos e aos bens públicos, como a proteção à saúde, ao meio ambiente e à segurança (COMISSÃO EUROPEIA, 2018b).

PARKES, 2019).

É necessário reconhecer que as campanhas de desinformação modernas foram potencializadas pelas novas tecnologias e aplicativos, como *smartphones* e mídias sociais (FIOTT; PARKES, 2019). Novas tecnologias podem ser usadas para disseminar a desinformação em uma escala e com uma velocidade e precisão sem precedentes. A internet aumentou enormemente o volume e a variedade de notícias disponíveis e mudou profundamente a maneira como as pessoas, os mais jovens em particular, acessam as notícias (COMISSÃO EUROPEIA, 2018b).

Existe uma vasta gama de fontes de notícias online, desde blogueiros a agências de notícias tradicionais, que podem facilmente influenciar grupos sociais e indivíduos (FIOTT; PARKES, 2019). Além disso, o uso de mídias sociais e fontes de notícias online permite que os autores de notícias falsas e desinformação executem suas atividades de forma anônima e a um custo mínimo (FIOTT; PARKES, 2019). Essa grande quantidade de mídias disponíveis também faz com que muitas pessoas fiquem confusas e nem sempre consigam discernir fato de ficção (LUCAS; POMERANTSEV, 2016).

As tecnologias de redes sociais são manipuladas para espalhar desinformação por meio de uma séria de etapas sequenciais: a **criação**, que pode envolver artigos escritos, complementados ou não por imagens ou vídeos fora do contexto, ou o emprego de novas tecnologias, inclusive baseadas em inteligência artificial, disponíveis para criar imagens e vídeos falsos, que permitem manipular a opinião pública com muito mais eficiência; a **amplificação**, que se aproveita de um terreno fértil para a disseminação da desinformação em mídias sociais e outras mídias online e faz uso de algoritmos,[37] de modelos de publicidade digital[38] e de tecnologias facilitadoras;[39] e a **divulgação** pelos usuários, que tendem a compartilhar os conteúdos sem nenhuma verificação (COMISSÃO EUROPEIA, 2018a).

Para ser eficaz, a desinformação deve atrair a atenção das pessoas, por meio de mensagens ou notícias provocativas, e levá-las a buscar informações adicionais em fóruns de comentários e discussões, de onde são conectadas a outras contas com mais notícias falsas. Essas pessoas comentam com amigos e familiares sobre essas notícias e assim elas se espalham

[37] Os algoritmos de critérios para priorizar a exibição de informações na internet são orientados pelo modelo de negócios das plataformas e pela maneira como isso privilegia o conteúdo personalizado e sensacionalista, que é, normalmente, mais provável de atrair a atenção e ser compartilhado entre os usuários. Ao facilitar o compartilhamento de conteúdo personalizado ente usuários com ideias semelhantes, os algoritmos aumentam indiretamente a polarização e fortalecem os efeitos da desinformação.

[38] Baseados, geralmente, em cliques, que recompensam conteúdo sensacionalista e viral. Esse modelo depende de redes de publicidade operadas por agências que garantem a veiculação em tempo real de anúncios com base na decisão de algoritmos.

[39] Tecnologias online, como serviços automatizados (conhecidos como “bots”), amplificam artificialmente a disseminação da desinformação. Esse mecanismo pode ser facilitado por perfis simulados (contas falsas) que não possuem um usuário autêntico por trás deles, sendo orquestrados, às vezes, em grande escala (chamadas de “fábricas de trolls”).

(FIOTT; PARKES, 2019). O alvo da desinformação não é o público em geral, mas as pessoas que já nutrem alguma desconfiança de seus sistemas, que estão procurando teorias ou informações, por mais ridículas que sejam, que corroborem suas suspeitas (LUCAS; POMERANTSEV, 2016).

O anonimato e a possibilidade de negação do ambiente virtual, com suas contas falsas e *spambots*, proporcionam uma camuflagem eficaz a ser explorada dentro de uma campanha híbrida. Da mesma forma, o baixo custo, o alcance e a velocidade da veiculação de ideias por meio das mídias sociais contribuíram para a revitalização da desinformação como uma ferramenta popular a ser empregada por atores híbridos (FIOTT; PARKES, 2019).

A liberdade de expressão pode ser explorada para disseminar a desinformação em uma sociedade. O efeito não é persuadir ou ganhar credibilidade, mas semear confusão por meio de teorias conspiratórias e proliferar falsidades (WEISS, 2014). Uma campanha de desinformação, aliada ao controle da informação, permite que vários aspectos importantes da Guerra Híbrida sejam alcançados, como a negação plausível e a interferência psicológica. Ela esconde os reais objetivos do ator híbrido, confunde o inimigo e sua sociedade, dificulta o dimensionamento da presença militar, confere flexibilidade para a escolha de métodos para escalar o conflito e cria cobertura para atividades militares dissimuladas (SNEGOVAYA, 2015).

Diversos fatores podem afetar o impacto que a desinformação terá sobre uma sociedade, como o seu nível de educação e cultura, a confiança percebida nas instituições e no governo e as desigualdades sociais e econômicas existentes (COMISSÃO EUROPEIA, 2018b). Um ator híbrido emprega a desinformação para poluir o espaço informacional, enfraquecer o debate democrático, fomentar insurreições e denegrir reputações (LUCAS; POMERANTSEV, 2016). Campanhas de desinformação promovem tensões sociais, polarização e desconfiança, corroem a confiança nas instituições e na mídia convencional e digital e limitam a habilidade dos cidadãos de tomarem decisões embasadas (COMISSÃO EUROPEIA, 2018b).

Dessa forma, concluímos que as campanhas de desinformação modernas foram potencializadas pelo desenvolvimento tecnológico, em particular pela internet e pelas mídias sociais, que as fizeram crescer em sofisticação, alcance, intensidade e impacto. Contudo, para ser eficaz, a desinformação deve explorar falhas existentes nas convicções das pessoas e no tecido político e social de um Estado para encontrar sustentação e prosperar. Ela busca controlar a narrativa dos fatos e, assim, confundir os demais atores, promover divisões internas, corroer a confiança nas instituições e limitar a capacidade de tomada de decisão.

2.7 Conclusões Parciais

O conceito da Guerra Híbrida foi desenvolvido a partir da análise da conduta de alguns atores não estatais em conflitos contemporâneos. Ele compreendia, inicialmente, o emprego não convencional de diversas capacidades, táticas e meios, buscando alcançar efeitos sinérgicos nas dimensões físicas e psicológicas do conflito. Sua caraterística principal era a capacidade de mesclar uma elevada sofisticação militar com habilidades não convencionais e o emprego eficaz de meios não militares, como a criminalidade, o terrorismo, instrumentos legais, ataques cibernéticos e a desinformação.

Contudo, a campanha da Rússia na Ucrânia trouxe uma nova perspectiva ao conceito, que evoluiu, passando a focar na potencialização dos efeitos alcançados pela maior disponibilidades de meios militares e não militares a serem empregados e na maior capacidade de coordenação que os Estados possuem. Nesse contexto, a ambiguidade, obtida por meio de ações projetadas para evitar os limites para resposta estabelecidos e da negação plausível, surge como uma característica importante.

A Guerra Híbrida pode, então, ser definida como o emprego sincronizado de múltiplos instrumentos do poder adaptados a vulnerabilidades específicas em todo o espectro de funções da sociedade para atingir efeitos sinérgicos. A seleção dos meios e de sua intensidade pode, então, ser representada graficamente, caracterizando a escalada horizontal e vertical das ações. A conjugação dos esforços pode gerar efeitos multiplicadores de força e contribuir para a ambiguidade.

Verificamos que, na Guerra Híbrida, um ator pode se valer de uma grande variedade de recursos para implementar sua estratégia. Em particular, a Guerra de Informação tem se mostrado uma poderosa ferramenta para o domínio do espaço cognitivo e psicológico. A evolução dos meios de comunicação tem tornado cada vez mais eficaz o emprego da informação como uma arma. As ações da Rússia na Ucrânia foram um exemplo da contribuição que a Guerra da Informação pode dar dentro da estratégia mais ampla da Guerra Híbrida.

Nesse contexto, a desinformação é uma ferramenta importante para moldar a percepção dos envolvidos. As campanhas de desinformação modernas foram potencializadas pelo desenvolvimento tecnológico, em particular pela internet e pelas mídias sociais, que as fizeram crescer em sofisticação, alcance, intensidade e impacto. Contudo, para ser eficaz, a desinformação deve explorar falhas existentes nas convicções das pessoas e no tecido político e social de um Estado para encontrar sustentação e prosperar. Por meio da desinformação, pode-se controlar a narrativa dos fatos e, assim, confundir os demais atores, promover divisões

internas, corroer a confiança nas instituições e limitar a capacidade de tomada de decisão.

3 COMBATENDO A GUERRA HÍBRIDA

Para muitos estudiosos, as ações de Guerra Híbrida são uma realidade do ambiente de segurança atual, principalmente na Europa e nos EUA (JOPLING, 2018)[40] e são uma tendência para o futuro.[41] Assim sendo, torna-se necessário que os Estados se preparem para lidar com essa realidade, ajustando suas estruturas e desenvolvendo estratégias específicas para essa ameaça, que também não poderão se limitar ao poder militar. Um dos desafios nesse sentido é identificar a ação, posicioná-la nessa larga faixa ocupada pela Guerra Híbrida e decidir o que fazer (MCDC, 2019).

De modo a apresentar uma base científica que possa orientar a formulação de uma estratégia nacional de combate à Guerra Híbrida, abordaremos, neste capítulo, o modelo desenvolvido pelo MCDC(CHW) *Project* em 2019. Para facilitar a compreensão do modelo teórico e associá-lo a medidas concretas a serem implementadas, traçaremos um paralelo, ao longo do capítulo, entre o modelo desenvolvido pelo MCDC e a estratégia adotada, em 2016, pela UE para combater a Guerra Híbrida (COMISSÃO EUROPEIA, 2016), identificando como as ações propostas nessa iniciativa se encaixam no modelo estudado.

Essa estratégia foi uma resposta da UE ao comportamento agressivo da Rússia, particularmente por suas ações na Ucrânia em 2014 (FIOTT; PARKES, 2019). O acompanhamento da implementação da estratégia europeia foi feito por meio de relatórios anuais em 2017 (COMISSÃO EUROPEIA, 2017), 2018 (COMISSÃO EUROPEIA, 2018d) e 2019 (COMISSÃO EUROPEIA, 2019), que apresentaram, também, ações adicionais incorporadas à estratégia.

3.1 O Modelo Desenvolvido pelo MCDC *Countering Hybrid Warfare Project*

O *MCDC(CHW) Project* é uma iniciativa multinacional, com base no Reino Unido, que busca auxiliar líderes nacionais e multinacionais, responsáveis pelas tomadas de decisão na área de segurança e defesa, a entender e a combater à Guerra Híbrida.[42] Como forma de orientar a formulação de políticas e estratégias para esse fim, foi desenvolvido um modelo para o

[40] Disponível em: <https://www.nato-pa.int/download-file?filename=sites/default/files/2018-12/166%20CDS%2018%20E%20fin%20-%20HYBRID%20THREATS%20-%20JOPLING_0.pdf>.

[41] Como pode ser observado na Estratégia de Segurança Nacional da Espanha, 2017 e no documento do Ministério da Defesa do Reino Unido: *Global Strategic Trends – The Future Starts Today, 2018*.

[42] Página do site oficial. Disponível em: <https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare>.

combate à Guerra Híbrida.[43]

Esse modelo é a segunda fase de um projeto que buscou estabelecer, inicialmente, uma compreensão comum sobre a Guerra Híbrida para, em seguida, elaborar uma orientação conceitual sobre como combatê-la. Ele foi desenvolvido a partir de pesquisas e análises, conduzidas por estudiosos dos países contribuintes, e da condução de estudos de caso. As principais ideias e conceitos decorrentes desses estudos foram então refinados em uma série de workshops e resultaram no modelo que será apresentado.

Como ilustrado na FIG. 3 abaixo, esse modelo foi estruturado em três componentes principais: a detecção de ameaças ou ataques híbridos; a dissuasão do agressor híbrido;[44] e a resposta a ataques híbridos (MCDC, 2019). Para orientar a implementação desses componentes, o modelo prevê, ainda, que sejam previamente definidos objetivos estratégicos realistas e limites para resposta[45] apropriados (MCDC, 2019), que serão aprofundados no APÊNDICE C – Estabelecendo objetivos estratégicos e limites para resposta. Para melhor compreender a dinâmica do modelo apresentado, será feita, a seguir, a apresentação de cada um desses elementos e de como eles podem ser explorados em uma estratégia para combater a Guerra Híbrida.

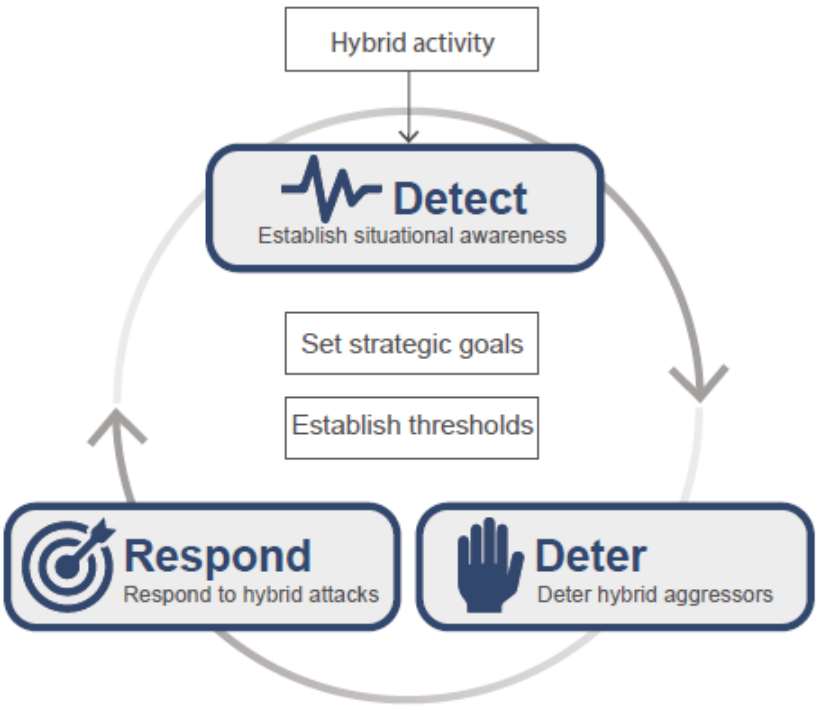

FIGURA 3: Modelo para combater a Guerra Híbrida
Fonte: MCDC, 2019, p. 22.

[43] Do original *Countering Hybrid Warfare Framework*, tradução nossa.
[44] Neste trabalho, os termos em inglês "deter" e "deterrence" encontrados no modelo estudado foram traduzidos e interpretados como dissuadir e dissuasão, respectivamente.
[45] Do original *thresholds*, tradução nossa.

3.2 – Detectar

Uma vez estabelecidos os objetivos estratégicos e os limites para resposta, o próximo passo para combater a Guerra Híbrida, e talvez o mais difícil, é identificar a ameaça (MCDC, 2019). Os limites para resposta fornecem um indicador extremo ou limite para a tomada de decisão. Contudo, as ações de um agressor híbrido poderão estar distribuídas, dentro de uma escalada horizontal, por todo o domínio PMESII e a intensidade das ações poderá estar abaixo dos limites de resposta estabelecidos, ou poderão cruzar esses limites e depois retrair, dificultando a formação de uma consciência situacional precisa, necessária à tomada de decisão. Diante dessas dificuldades, há necessidade de se buscar novas abordagens para orientar o desenvolvimento da atividade de inteligência que permita a detecção de ameaças e ataques híbridos.

De acordo com o documento em pauta, os métodos tradicionais de detecção de ameaças, centrados no inimigo, perdem sua eficácia quando empregados em um cenário de Guerra Híbrida (MCDC, 2019). Esses métodos, enquadrados no conceito de inteligência de alerta,[46] baseiam-se no emprego de indicadores, que são monitorados para estabelecer o padrão das atividades normais do inimigo para, posteriormente, reconhecer mudanças relevantes que possam fornecer um alerta antecipado (MCDC, 2019). Por várias razões, esses indicadores tendem a focar nos aspectos militares dos atores, como sua força, capacidades e atividades (GRABO, CYNTHIA *apud* MCDC, 2019).[47]

Embora esse tipo de indicador continue importante, a ênfase da Guerra Híbrida em criar e explorar a ambiguidade, combinada com o emprego de meios não militares, torna necessário levar a inteligência de alerta além dessa abordagem unidimensional e criar processos e métodos que permitam a detecção de atividades híbridas direcionadas às vulnerabilidades críticas da sociedade (MCDC, 2019). Para essa situação, não bastará estabelecer novos indicadores, uma vez que seria bastante difícil prever quais meios seriam empregados contra quais vulnerabilidades (MCDC, 2019).

Outra dificuldade apresentada para a inteligência de alerta, pelas características da Guerra Híbrida, é a origem e a natureza variadas das informações necessárias para a montagem de um quadro claro da situação que se apresenta. Uma vez que as ações dos agressores híbridos poderão se dar nos domínios das diversas funções críticas de uma sociedade, o

[46] Do original *Warning Intelligence*, tradução nossa. O termo se refere a atividades de inteligência que detectam e informam desenvolvimentos sensíveis ao tempo que advertem quanto a ações ou intenções hostis (MCDC, 2019, p 25).
[47] GRABO, Cynthia. *Handbook of Warning Intelligence, Rowman and Littlefield,* 2015.

compartilhamento e análise das informações desses domínios será necessário para a compreensão do cenário que se está enfrentando. Além disso, a identificação e interpretação dessas informações vai requerer a participação de analistas com conhecimento dos aspectos específicos dessas diversas áreas e não somente do campo militar.

Faz-se necessário, então, expandir o desenvolvimento de indicadores e buscar novas abordagens para identificar ameaças ambíguas. Para lidar com esses desafios, o estudo propõe mudanças na forma de conduzir a inteligência de alerta para a Guerra Híbrida, apresentado dois processos distintos para identificar as ameaças (MCDC, 2019).

O primeiro processo seria o monitoramento do ambiente, com o auxílio de indicadores ajustados ao contexto híbrido, para identificar informações que permitam esclarecer "incógnitas conhecidas"[48] sobre possíveis ataques, ou seja, aquelas lacunas de conhecimento que já se sabe que existem (MCDC, 2019).

O segundo processo está relacionado à descoberta de "incógnitas desconhecidas",[49] o que envolve a captura e a interpretação correta de informações relacionadas a uma ação adversa potencialmente hostil que não foi concebida anteriormente (MCDC, 2019). Nesse último caso, não é possível realizar o monitoramento de indicadores para identificar mudanças de padrões conhecidos, porque não há padrões conhecidos. É necessário mapear o ambiente para detectar anomalias não antecipadas e reconhecer padrões anteriormente não vistos (MCDC, 2019).

Para facilitar a compreensão e distinção entre esses dois processos, abordaremos quatro estudos de caso que ilustram os conceitos acima.

3.2.1 – Iniciativas para Adaptar a Inteligência de Alerta para a Guerra Híbrida

Exemplos das mudanças propostas são demonstrados no estudo do MCDC pela apresentação da visão geral de quatro estudos de caso onde foram adotadas iniciativas para desenvolver alertas antecipados de atividades híbridas. No caso do monitoramento, foram realizadas a ampliação da abrangência dos métodos de inteligência de alerta e o deslocamento dos indicadores para a esquerda do Continuum do Conflito (MCDC, 2019). Para a descoberta de ameaças totalmente desconhecidas, foram criadas alternativas para descobrir novos padrões

[48] Do original *Known unknowns*, tradução nossa. Formas ou modos de ataque híbrido que nós sabemos que são desconhecidos. (MCDC, 2019, p 26)

[49] Do original *Unknown unknowns*, tradução nossa. Riscos relacionados a ataques híbridos que podem existir onde não se tem consciência de sua natureza, das nossas vulnerabilidades a eles ou mesmo quanto a nossa própria ignorância sobre essas ameaças. (MCDC, 2019, p 26)

e o mapeamento de influências (MCDC, 2019).

A ampliação da abrangência foi adotada pelo governo da Áustria e visa a antecipar o emprego de meios não militares de ataque por meio da identificação das vulnerabilidades nacionais críticas, sua associação a supostos objetivos e capacidades do adversário e o desenvolvimento de indicadores que consigam conectar esses dois fatores (MCDC, 2019). Conforme citado anteriormente, a criação e interpretação desses novos indicadores, para todas as funções críticas da sociedade, irá requerer a participação de especialistas de todas as áreas do governo e, se possível, do setor privado (por exemplo, do setor bancário e da mídia).

Já os EUA expandiram a inteligência de alerta para faixas de menor intensidade dentro do Continuum do Conflito, com o desenvolvimento de indicadores para atividades que, normalmente, se situariam bem abaixo dos limites para resposta de conflitos convencionais (MCDC, 2019). Com isso, buscaram identificar ameaças que, anteriormente, seriam consideradas sem relevância para serem monitoradas. Esse ajuste é, especialmente, desejável quando do emprego de meios não militares por ameaças híbridas.

Em uma outra vertente, a identificação de novos padrões procura compensar a incapacidade de se estabelecer indicadores para as “incógnitas desconhecidas”, pelo mapeamento de anomalias em atividades que afetam vulnerabilidades críticas e que possam indicar certa ambiguidade nos efeitos desejados (MCDC, 2019). Essas anomalias vão se constituir em pequenos indícios, como peças de um quebra-cabeças, que poderão indicar a existência de um ataque híbrido. Esses indícios poderão aparecer em várias áreas da sociedade, exigindo a integração horizontal dos setores do governo e, mais uma vez, de entidades civis. Assim, no caso apresentado, foi criada uma estrutura próxima ao mais alto escalão do governo finlandês para facilitar a troca e a análise das informações (MCDC, 2019).

Por fim, o mapeamento de influências foi adotado pelo Reino Unido por meio da criação de uma ferramenta, no Ministério da Defesa, que permite o monitoramento de fontes abertas para tentar identificar mecanismos de influência sendo empregados em atividades híbridas (MCDC, 2019). Esses mecanismos são, então, avaliados de acordo com seu nível de influência e o impacto da sua influência e os resultados obtidos são comparados com um parâmetro considerado normal (MCDC, 2019).

As quatro iniciativas tratadas acima apresentam abordagens para o problema da detecção de ameaças híbridas que podem ser aproveitadas em esforços futuros para melhorar a capacidade de alerta antecipado contra a Guerra Híbrida. Elas envolvem o desenvolvimento de novos tipos de indicadores, o reposicionamento desses indicadores e a varredura do ambiente para identificar variações que, isoladamente, podem não trazer um significado específico, mas

que, quando analisadas em conjunto com outras variações, proporcionam a percepção real da ameaça. A seguir, veremos as ações adotadas pelo União Europeia para detectar ameaças híbridas.

3.2.2 – A Detecção na Estratégia da União Europeia

Dentro da estratégia da União Europeia para combater a Guerra Híbrida, o componente relativo à detecção de ameaças ou ataques híbridos está estruturado em duas vertentes: no reconhecimento da natureza híbrida de uma ameaça e no aprimoramento da consciência situacional (COMISSÃO EUROPEIA, 2016).

Nesse sentido, foi proposta a realização de pesquisas de risco para identificar vulnerabilidades que possam afetar as estruturas críticas dos Estados Membros. Com isso, busca-se "aprimorar a consciência situacional pelo monitoramento e avaliação dos riscos que podem ter como alvos as vulnerabilidades da UE" (COMISSÃO EUROPEIA, 2016, p. 3). A UE procurou apoiar essa atividade, desenvolvendo metodologias de avaliação de riscos de segurança personalizadas para cada Estado (COMISSÃO EUROPEIA, 2016). O resultado desse processo é a identificação de indicadores de ameaças híbridas que serão incorporados a mecanismos de alerta antecipado (COMISSÃO EUROPEIA, 2016).

Outra ação importante, foi a criação, dentro de uma das estruturas de inteligência da UE,[50] de uma plataforma para a "fusão" de informações relacionadas a ameaças híbridas, espalhadas em diversos lugares da estrutura administrativa da UE e dos Estados Membros, e para o seu compartilhamento com os setores pertinentes. A *EU Hybrid Fusion Cell*[51] é capaz de analisar informações sigilosas e de fontes abertas para identificar mudanças no ambiente de segurança relacionadas a atividades híbridas e preparar assessoramentos em apoio à tomada de decisão (COMISSÃO EUROPEIA, 2016)**.**

Essa célula de inteligência oferece um ponto focal para a atividade de inteligência contra a Guerra Híbrida e facilita o intercâmbio e o compartilhamento de informações entre setores que, normalmente, não estariam integrados na atividade de inteligência estratégica, como o social, o de infraestrutura e o financeiro. Para isso, deve ser composta por especialistas militares e civis de áreas relacionadas à Guerra Híbrida (economia, social, infraestrutura, mídia, cibernética, entre outras), trabalha em estreita coordenação com outros órgãos de inteligência e mantém pontos de contato junto aos Estados Membros e a outros setores dentro da UE

[50] *EU Intelligence and Situation Centre* (EU INTCEN) (Centro de inteligência e Situação da UE, tradução nossa).
[51] Célula de Fusão Híbrida da UE, tradução nossa.

(COMISSÃO EUROPEIA, 2016). Além de assessorar, essa agência também prepara diversos produtos voltados à melhoraria da conscientização dos diversos setores do governo quanto ameaças híbridas em potencial (COMISSÃO EUROPEIA, 2016).

Nos relatórios subsequentes, referentes à implementação dessa estratégica,[52] fica clara a importância dada pela UE à implementação dessas duas medidas. Para a avaliação do risco e das vulnerabilidades das infraestruturas críticas, foi estabelecida uma comissão com especialistas de diversas áreas para formular uma pesquisa com aspectos comuns a todos os Estados Membros.[53] Essa pesquisa foi aplicada a partir do final de 2017 e, até o relatório de 2019, 24 Estados Membros já a haviam respondido. Com os resultados dessa pesquisa, a UE já havia começado a identificar indicadores de atividade híbrida e a formular recomendações para políticas.

Já a *EU Hybrid Fusion Cell* tornou-se totalmente operacional em 2017 (COMISSÃO EUROPEIA, 2018d). Desde então, tem participado ativamente dos debates relacionados à conscientização sobre as ameaças híbridas (COMISSÃO EUROPEIA, 2019). Ainda segundo os relatórios anuais, sua ativação conseguiu melhorar o fluxo de informações sobre essas ameaças, principalmente com o estabelecimento de pontos de contato nos Estados Membros e de sua aproximação com *European Centre of Excelence for Countering Hybrid Threats*.

Essas duas medidas adotadas pela UE estão aderentes ao proposto no modelo do MCDC, uma vez que se valem das pesquisas de risco para estabelecer novos indicadores que ajudam a identificar ações híbridas. Da mesma forma, a criação da *EU Hybrid Fusion Cell* mostra a preocupação com a análise de dados que, anteriormente, estariam desassociados ou que, por si só, não teriam relevância devido à sua natureza ou intensidade.

Analisando as avaliações dos relatórios anuais, fica evidente que essas medidas aprimoraram a capacidade de detecção de atividades atípicas, que podem estar relacionadas à Guerra Híbrida. Principalmente, a melhoria da capacidade de inteligência para analisar ações difusas em áreas diversas e reconhecer um padrão comum entre elas. Contudo, esse é apenas a etapa inicial em uma estratégia de combate à Guerra Híbrida. O próximo passo é adotar ações para se contrapor a esse tipo de ameaça. Para entender melhor esse processo, será abordada agora a segunda componente do modelo do MCDC(CHW) *Project*: a dissuasão.

[52] COMISSÃO EUROPEIA 2017, 2018d, 2019.
[53] Denominada "*Friends of Presidency Group"* (Grupo dos Amigos do Presidente, tradução nossa).

3.3 – Dissuadir

"A dissuasão talvez seja a ferramenta mais importante para combater a Guerra Híbrida, simplesmente porque ela pode, antes de mais nada, impedir a ocorrência de ataques" (MCDC, 2019, p. 35, tradução nossa).

Segundo o Glossário das Forças Armadas, dissuasão "é a atitude estratégica que, por intermédio de meios de qualquer natureza, inclusive militares, tem por finalidade desaconselhar ou desviar adversários, reais ou potenciais, de possíveis ou presumíveis propósitos bélicos" (MD35-G-01, 2015, p 93). Segundo Couto (1988), ela é decorrente da capacidade[54] e da credibilidade[55] de um ator, mas depende também da fidelidade de comunicação.[56]

As estratégias de dissuasão podem ser divididas em duas grandes categorias: a dissuasão por negação (ou defensiva) e por punição (MCDC, 2019). A dissuasão por negação baseia-se em convencer um adversário de que ele não conseguirá atingir seus objetivos, em decorrência de nossas ações. Já a dissuasão por punição baseia-se na ameaça de retaliação, persuadindo o adversário de que a manutenção de ações agressivas teria um custo proibitivo.[57]

De acordo com o estudo do MCDC, a Guerra Híbrida apresenta características que desafiam os pilares da dissuasão. O emprego de múltiplos instrumentos do poder (MPECI),[58] direcionados a diversas vulnerabilidades, em um ataque sincronizado e multimodal, com ênfase na criatividade e na ambiguidade, dificulta o processo de tomada de decisão necessário a dar credibilidade às ações, enfraquece a capacidade de resposta por meios não militares e tornam a comunicação incerta pela dificuldade de compreender o que está acontecendo (MCDC, 2019). Tais aspectos fazem com que a dissuasão de agressores híbridos – a dissuasão híbrida – assuma, também, características próprias.

Para compensar esses fatores, MCDC(CHW) *Project* explorou desenvolvimentos recentes na teoria da dissuasão, como a Dissuasão de Quarta Onda[59] e a Dissuasão

[54] A habilidade ou capacidade técnica de executar ações que imporão custos ao adversário (MCDC, 2019, p. 35, tradução nossa).
[55] A vontade de executar ações que imporão custos ao adversário (MCDC, 2019, p 35, tradução nossa).
[56] O entendimento e a percepção de duas vias que informa a relação custo-benefício de ambos os lados (MCDC, 2019, p 35, tradução nossa).
[57] GRAY, Colin S. (2003) – Maintaining Effective Deterrence.
[58] Organizados nos campos militar, político, econômico, civil e informacional (MPECI) (MCDC, 2019, tradução nossa).
[59] Teoria caracterizada por dois elementos relevantes para a Guerra Híbrida: a inclusão da dissuasão a ameaças assimétricas de atores não estatais; e o reconhecimento de um conceito mais amplo de dissuasão que vai além dos meios militares (MCDC, 2019).

Cibernética,[60] em estudos e workshops, de modo a chegar a um **conjunto de cinco princípios para dissuadir agressores híbridos** (MCDC, 2019):

a) A dissuasão tradicional[61] permanece vital contra agressões armadas e deve ser mantida.

b) Agressores híbridos podem ser dissuadidos pelo emprego de medidas específicas. Para isso, deve-se ter em conta que (MCDC, 2019):

– é possível, até certo ponto, discernir a intensão e a capacidade de um adversário;

– é possível atribuir a responsabilidade pelos meios usados em ataque híbrido, apesar da ambiguidade;

– sempre há medidas que podem ser adotadas; e

– agressores híbridos possuem vulnerabilidades que também podem ser exploradas.

c) Os princípios da dissuasão devem ser interpretados de maneira diferente na Guerra Híbrida:

– para se obter **credibilidade**, é necessário demonstrar determinação e agir sem hesitação, empregando todos os instrumentos do poder em ações de baixa intensidade (MCDC, 2019);

– ampliar as **capacidades**, melhorando os métodos de detecção; aprimorando e expandindo ferramentas para solucionar as vulnerabilidades e executar ações contra os agressores; e desenvolvendo mecanismos e uma cultura que facilitem a coordenação dentro de uma resposta do governo como um todo (MCDC, 2019); e

– facilitar a **comunicação**, estabelecendo limites para dissuasão e resposta claros, realistas e bem ajustados e avaliando a mensagem a ser passada com a divulgação ou não desses limites (MCDC, 2019).

d) Apesar da resiliência ser um fator importante da dissuasão por negação, pode ser que ela não seja suficiente para evitar ataques híbridos. A dissuasão híbrida requer equilíbrio entre medidas de negação e punição (MCDC, 2019); e

e) Busque uma abordagem ajustada ao agressor híbrido, desagregando sua estratégia nas diversas ações que a compõem e atacando os elementos específicos de sua campanha. Com isso, busca-se obter ganhos marginais, atacando os fatores que tornam a campanha possível, empregando os meios que lhe conferem maior credibilidade e com foco nos objetivos, motivações e vulnerabilidades dos atores (MCDC, 2019).

---

[60] O contexto envolve a aplicação de meios tecnológicos não militares para obter influência e ameaçar danos. Ver ANDRES, Richard. "Cyber Gray Space Deterrence". PRISM, volume 7, n. 2, pag. 91-98. 2010. Disponível em: <https://cco.ndu.edu/PRISM-7-2/Article/1401927/cyber-gray-space-deterrence/>.

[61] Empregada para se referir à dissuasão por meios convencionais, nucleares e modernos (como a cibernética).

Devido às características da Guerra Híbrida já citadas anteriormente, a dissuasão tradicional, apesar de permanecer válida, apresenta deficiências para deter ataques híbridos, principalmente de baixa intensidade. Assim, com base nos outros quatro princípios apresentados acima, o modelo apresenta propostas atualizadas para a dissuasão híbrida, que serão vistas no próximo item.

No caso da dissuasão por negação, um componente chave é abordar as vulnerabilidades existentes em todo o governo e na sociedade, em todo o espectro de suas funções críticas de modo a impedir ou, pelo menos, dificultar sua exploração. Segundo o estudo do MCDC, alguns países já vêm adotando essa abordagem em suas estratégias de resiliência.[62] Já a dissuasão por punição deve explorar todos os meios disponíveis nos instrumentos do poder nacional, dentro do conceito de escalada horizontal, direcionados a vulnerabilidades identificadas nos agressores híbridos (MCDC, 2019).

O estudo realizado pelo MCDC apresenta medidas que podem ser aplicadas às funções críticas da sociedade, organizadas nos domínios PMESII, para aumentar a resiliência e minimizar os efeitos de ataques híbridos. O APÊNDICE D – Ações para dissuadir agressores híbridos traz uma relação dessas medidas.

3.3.1 – A Dissuasão na Estratégia da União Europeia

Dentro da estratégia da UE para combater a Guerra Híbrida, a dissuasão tem um papel fundamental. Das vinte e duas ações propostas na estratégia, dezesseis estão relacionadas com esse componente, basicamente envolvendo a construção da resiliência na sociedade e para o funcionamento do Estado, mas também a compreensão do fenômeno, sua divulgação e a busca por estratégias específicas.

Justamente no que tange à compreensão da Guerra Híbrida e à formulação de estratégias setoriais para combatê-la, foi estabelecido o Centro de Excelência Europeu para Combater Ameaças Híbridas em 2017, na Finlândia, que já conta com 22 membros. Seu foco está na pesquisa de como estratégias híbridas têm sido aplicadas e no desenvolvimento de novos conceitos e tecnologias para aumentar a resiliência e a capacidade de resposta (COMISSÃO EUROPEIA, 2016).

Esse centro funciona em estreita coordenação com outros centros de excelência da UE e da OTAN, em áreas como defesa cibernética, comunicação estratégica e cooperação civil

[62] Suécia (“Total Defense”), Noruega (“Support and Cooperation”), Finlândia (“Comprehensive Security”), Áustria (“Comprehensive National Dfense”) e Singapura (“Total Defense”).

e militar, de modo a se beneficiar de insights que possam ser aplicados ao combate à Guerra Híbrida (COMISSÃO EUROPEIA, 2016). Entre os produtos produzidos, encontram-se estudos e análises sobre o assunto, seminários, workshops, conferências e a organização de treinamentos e exercícios (COMISSÃO EUROPEIA, 2018d, 2019).

A criação de um centro de excelência para melhor compreender o fenômeno da Guerra Híbrida também é aderente ao modelo proposto pelo MCDC, uma vez que possibilita adaptar os princípios da dissuasão às particularidades do ambiente híbrido. Assim, as ações desenvolvidas na estratégia europeia, que tem como base o aprimoramento da resiliência, terão maior probabilidade de alcançar o efeito dissuasório desejado.

Como dito anteriormente, a resiliência está no centro das ações da UE para enfrentar ataques híbridos. Ela prevê esforços em diversas áreas, como: a proteção da infraestrutura crítica;[63] a garantia da saúde pública e da segurança alimentar; o fortalecimento das capacidades de defesa; a segurança cibernética; o combate ao financiamento de ameaças híbridas; o combate à radicalização e ao extremismo violento; e a cooperação com outros países (COMISSÃO EUROPEIA, 2016). Esses esforços não são específicos para as ameaças de natureza híbrida, mas, certamente, tornam os Estados melhor preparados para enfrentá-las. Será feita, a seguir, uma rápida abordagem de cada uma dessas áreas:

a) De maneira geral, para aumentar a proteção e a **resiliência da infraestrutura crítica**, a UE determinou a identificação de ferramentas, incluindo indicadores, que possam ser empregadas contra ataques híbridos em diversos setores, além de reforçar programas e diretivas já existentes (COMISSÃO EUROPEIA, 2016), como o *European Program for Critical Infraestructure Protection*[64] e a *Directive on European Critical Infraestructure*.[65] Outro aspecto abordado foi a adoção de um regulamento para a triagem de investimentos diretos estrangeiros que possam afetar as infraestruturas e tecnologias críticas (incluindo a inteligência artificial, a segurança cibernética e de uso dual), o fornecimento de insumos críticos e o acesso à informação sensível ou a habilidade de controlá-la (COMISSÃO EUROPEIA, 2018d).

Para cada setor específico, avaliações dos riscos à segurança — incluindo os políticos, tecnológicos, comerciais, sociais, naturais, ataques cibernéticos, sabotagem e terrorismo — e a revisão de normas e regulamentos voltados à proteção e segurança das instalações e dos serviços e de prevenção e resposta a crises foram comuns a todos. Além dessas

[63] Infraestrutura de transportes, de energia e espacial (COMISSÃO EUROPEIA, 2016).
[64] Programa Europeu de Proteção das Infraestruturas Críticas, tradução nossa. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52006DC0786&from=EN>.
[65] Diretiva para a Infraestrutura Crítica Europeia, tradução nossa. Disponível em: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF>.

medidas comuns, foram propostas, também, ações direcionadas às particularidades de cada setor, como veremos a seguir.

No setor energético, a produção e distribuição são de vital importância e falhas significativas podem ter resultados prejudiciais e até catastróficos. Um elemento essencial da estratégia são os esforços para diversificar as fontes, fornecedores e rotas de distribuição de energia elétrica, gás e óleo (COMISSÃO EUROPEIA, 2016).

Naturalmente, especial atenção é dedicada aos materiais e instalações nucleares, que deverão adotar os mais elevados padrões de segurança (COMISSÃO EUROPEIA, 2018d). São propostas, também, diretrizes para o setor de defesa e segurança direcionadas à gestão sustentável, reduzindo sua "pegada energética" e tornando-o mais eficiente, com a adoção de energias mais limpas, como a eólica, a solar, os biocombustíveis e o aperfeiçoamento dos sistemas com o uso de redes inteligentes e armazenamento de energia (COMISSÃO EUROPEIA, 2018d).

No setor de transportes, aqui incluídos os transportes aéreos, terrestres — rodoviário e ferroviário — e marítimos, tanto de carga quanto de pessoas, por se tratarem de atividades em domínios diversos, as avaliações de risco e a atualização das legislações serão direcionadas a cada um desses domínios, embora possam haver aspectos comuns, como ameaças ao sistema de localização por satélite e a segurança cibernética (COMISSÃO EUROPEIA, 2016).

Outra preocupação comum é a modernização dos sistemas de informação sobre cargas para a melhoria da gestão de riscos aduaneiros (COMISSÃO EUROPEIA, 2017). A capacidade de detecção da entrada ilegal de materiais Nuclear, Biológico, Químico e Radiológicos (NBQR) também deve ser foco de aprimoramento diante da possibilidade de emprego por agressores híbridos (COMISSÃO EUROPEIA, 2018d).

Por fim, ainda dentro da proteção à infraestrutura crítica, a resiliência da infraestrutura espacial é vital para o funcionamento dos serviços satelitais. O atraso gerado no desenvolvimento do programa espacial brasileiro decorrente do acidente que causou a explosão no Centro de Lançamento de Alcântara, em 2003, ilustra bem os danos que ações contra esse tipo de infraestrutura podem acarretar.

Assim, UE vem desenvolvendo várias ações nessa área para garantir a disponibilidade da infraestrutura, de facilidades e de serviços à longo prazo, para proteger o fornecimento de dados do espaço e para garantir o acesso seguro a comunicações por satélite (COMISSÃO EUROPEIA, 2018d). Nesse sentido, percebe-se uma grande preocupação com a obtenção e manutenção de autonomia na área espacial como um fator de segurança para os

Estados, em particular contra ameaças híbridas.

Conforme demonstrado neste subitem, a infraestrutura crítica de um Estado abrange uma vasta gama de setores e serviços. Naturalmente, qualquer ataque direcionado a essas instalações teria um grande potencial de danos e poderia ser usado de diversas maneiras, entre elas criar insatisfação contra o governo, criar confusão na sociedade ou enfraquecer a capacidade de resposta do governo. Para evitar que isso aconteça, é fundamental que o Estado aborde essa questão a fundo e de maneira gradual e consistente, pois são ações que não trarão resultado em um curto espaço de tempo.

b) A segunda área considerada na estratégia europeia para o aprimoramento da resiliência é a proteção à saúde pública e à segurança alimentar (COMISSÃO EUROPEIA, 2016). O exemplo atual da COVID-19 mostra claramente os efeitos disruptivos que podem ser gerados na sociedade e na economia pela disseminação de doenças infectocontagiosas, pela contaminação por agentes NBQR ou pela propagação de doenças animais e pragas vegetais.

Assim, a estratégia prevê o emprego de mecanismos já existentes de segurança sanitária e alimentar e de proteção ambiental para melhorar a conscientização e a resiliência nessas áreas (COMISSÃO EUROPEIA, 2016). Também é importante o estabelecimento de sistemas de alerta antecipado e resposta, que sejam testados periodicamente. Exemplo disso foi o exercício CHIMERA, realizado em 2018, onde um cenário fictício envolveu a liberação de uma doença transmissível combinada com ataques cibernéticos sobre a infraestrutura crítica de saúde, incluindo hospitais (COMISSÃO EUROPEIA, 2018d).

c) Outro elemento importante da dissuasão são as Forças Armadas de um Estado ou, em uma visão mais abrangente, sua capacidade de defesa (COMISSÃO EUROPEIA, 2016). Nesse sentido, a estratégia europeia prevê o fortalecimento das capacidades de defesa pela atualização do planejamento de força baseado em capacidades, com base na avaliação dos resultados de exercícios construídos dentro de um cenário de uma ameaça híbrida (COMISSÃO EUROPEIA, 2017). Outra contribuição do setor de defesa para o combate à Guerra Híbrida envolve o fortalecimento da base industrial e tecnológica de defesa, com o desenvolvimento das capacidades identificadas nos domínios híbridos e na busca pela autonomia tecnológica (COMISSÃO EUROPEIA, 2019).

d) A quarta área a ter sua resiliência aprimorada é a da segurança cibernética. A dependência cada vez maior das soluções de TI para o funcionamento tanto do setor público quanto do setor privado e a dificuldade para determinar a autoria das ações no domínio cibernético tornam a realização de ataques cibernéticos, para interromper ou comprometer os serviços digitais, uma ferramenta ideal para um agressor híbrido. Assim, as ações relacionadas

à segurança cibernética são fundamentais para a construção da resiliência.

Dentro da estratégia europeia, boa parte dessas ações estão voltadas para o desenvolvimento e implementação de estratégias e diretivas. Como exemplo, podem ser citadas a *Network and Information Services Directive*,[66] que trata dos riscos relacionados a provedores de serviços essenciais (COMISSÃO EUROPEIA, 2016), o *Joint Communication on Resilience, Deterrence and Defense: Building Strong Cybersecurity in Europe*,[67] com medidas que buscam dar maior impulso às capacidades e estruturas de segurança cibernética, e o *Cybersecurity Act*,[68] para orientar as ações dos setores e melhorar a eficácia de respostas intersetoriais (COMISSÃO EUROPEIA, 2019).

Para aumentar a resiliência de usuários e da infraestrutura contra ataques cibernéticos e híbridos, a estratégia europeia ressalta a necessidade de se trabalhar junto com a indústria, por meio de parcerias público privadas, com foco na pesquisa e inovação para o desenvolvimento de produtos e serviços (COMISSÃO EUROPEIA, 2016). Prevê, também, orientações específicas para o setor energético,[69] de transportes e financeiro (COMISSÃO EUROPEIA, 2016).

Por fim, para melhorar a identificação e resposta a ameaças, a estratégia europeia incentiva a cooperação entre setores, por meio da troca de informações e boas práticas (COMISSÃO EUROPEIA, 2016), a realização de exercícios cibernéticos (COMISSÃO EUROPEIA, 2018d) e o emprego de equipes de resposta a incidentes,[70] nos níveis setorial e nacional (COMISSÃO EUROPEIA, 2019).

A vertente cibernética é um caso típico em que a dissuasão tradicional tem que ser adaptada para o contexto híbrido. Como abordado no capítulo anterior, a realização de ataques cibernéticos e a desinformação são duas das ferramentas que trouxeram um novo alcance ao emprego de meios não militares nos conflitos, por atores estatais e não estatais. Dessa forma, qualquer estratégia para enfrentar a Guerra Híbrida deve dar especial atenção a esse aspecto da resiliência.

e) Uma área que, muitas vezes, não é associada quando se pensa em dissuasão e

---

[66] Diretiva para Serviços de Rede e da Informação, tradução nossa. Disponível em: <https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=CELEX%3A32016L1148>.

[67] Comunicado Conjunto sobre Resiliência, Dissuasão, e Defesa: Construção de uma Segurança Cibernética Forte na Europa, tradução nossa. Disponível em: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450>.

[68] Lei da Segurança Cibernética, tradução nossa. Disponível em: <https://eur-lex.europa.eu/eli/reg/2019/881/oj>.

[69] *Recommendation on Cybersecurity in the Energy Sector* (Recomendações sobre Segurança Cibernética para o Setor de Energia, tradução nossa). Disponível em: <https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf>.

[70] *Computer Security Incidents Response Teams* (Equipes de Resposta a Incidentes de Segurança Computacional, tradução nossa).

resiliência é o combate ao financiamento do terrorismo e à lavagem de dinheiro (COMISSÃO EUROPEIA, 2016). Uma vez que agressores híbridos podem apoiar financeiramente grupos terroristas, organizações criminosas, grupos de pressão ou partidos políticos favoráveis a suas causas, a UE vem estabelecendo mecanismos que permitam identificar e rastrear as movimentações financeiras suspeitas e facilitar a troca de informações entre os diversos órgãos envolvidos (COMISSÃO EUROPEIA, 2016).

f) Além das componentes materiais, a resiliência da sociedade como um todo também deve ser buscada. Assim, ações para evitar o surgimento ou o agravamento de tensões sociais devem ser adotadas, uma vez que divisões religiosas ou ideológicas, conflitos étnicos ou contra minorias podem ser explorados por um agressor híbrido.

Nesse sentido, a estratégia da UE estabelece ações para combater a radicalização e o extremismo violento (COMISSÃO EUROPEIA, 2016). Além do combate ao financiamento, a UE criou um grupo de especialistas em radicalismo[71] para "prover recomendações na coordenação, alcance e impacto das políticas de prevenção" (COMISSÃO EUROPEIA, 2018d, p. 10) e tem buscado lidar com questões econômicas, políticas e sociais que possam se tornar motivo de polarização social (COMISSÃO EUROPEIA, 2017). Aliada a isso, a promoção de uma educação inclusiva e de valores comuns, que transmitam o respeito às diferenças e a tolerância, podem contribuir para fortalecer a sociedade (COMISSÃO EUROPEIA, 2017).

Um aspecto importante da resiliência contra essas ameaças é o combate à desinformação e à propaganda, usados, como abordado no capítulo anterior, para manipular indivíduos ou grupos sociais, recrutar membros e incentivar o extremismo. Para se opor a essas iniciativas, a UE tem focado na comunicação estratégica para desconstituir as narrativas falsas, expor suas origens e o interesses envolvidos, para aumentar a conscientização da população e torná-la menos susceptível a essas influências (COMISSÃO EUROPEIA, 2016). Ao mesmo tempo, a UE tem procurado reduzir a disponibilidade de material, principalmente online, que faça apologia ao terrorismo, ao ódio e à intolerância, sem ferir os direitos fundamentais de liberdade de expressão e de acesso às informações (COMISSÃO EUROPEIA, 2017). Dentro do escopo deste trabalho, as ações adotadas pela UE para combater a desinformação abordadas em maior profundidade no próximo capítulo, junto com as ações propostas por outras estratégias.

g) Por último, dentro das medidas para aumentar a resiliência, a UE propõe aumentar a cooperação com outros países, auxiliando-os na construção de suas capacidades

[71] *High-Level Expert Group on Radicalization* (Grupo de Peritos de Alto Nível em Radicalização, tradução nossa).

para se protegerem de ameaças híbridas, de modo a evitar que esses países se tornem uma porta de entrada para essas ameaças.[72] A UE tem ajudado países vizinhos, por exemplo, com a aplicação de pesquisas de risco híbrido, de modo a permiti-los identificar suas vulnerabilidades.[73] Adicionalmente, tem procurado orientá-los na resolução das deficiências e fornecido apoio técnico e financeiro.

Todas as ações citadas neste subitem dão uma noção da dimensão das ações sendo conduzidas pela UE dentro de sua estratégia para combater a Guerra Híbrida. A dissuasão de ameaças, em particular as de natureza híbrida, requer que o Estado demonstre capacidade e credibilidade. Para isso, a UE aposta no fortalecimento da resiliência de sua sociedade e de suas funções críticas.

Ainda assim, mesmo que essas condições sejam alcançadas, outros atores podem se sentir motivados a agir contra os nossos interesses, empregando medidas mais assertivas para alcançar seus objetivos. Nesse caso, um Estado tem que ser capaz de responder a um ataque híbrido. Para isso, passaremos a abordar o terceiro componente do modelo do MCDC.

3.4 – Responder

No caso de a dissuasão falhar e um Estado vir a sofrer ataques híbridos, ele deve estar em condições de responder a esses ataques de modo a mudar o comportamento do agressor. Apesar da Guerra Híbrida buscar evitar respostas decisivas, dificultando a compreensão da situação e o processo de tomada de decisão, é possível ir além da dissuasão e adotar respostas mais diretas a essas ameaças. Para isso, o modelo proposto pelo MCDC apresenta um processo para organizar essa resposta, com base na seleção das formas e meios a serem empregados.[74] Esse processo está representado na FIG. 4, a seguir.

[72] COMISSÃO EUROPEIA, 2016.
[73] COMISSÃO EUROPEIA, 2017, 2018d e 2019.
[74] MCDC, 2019.

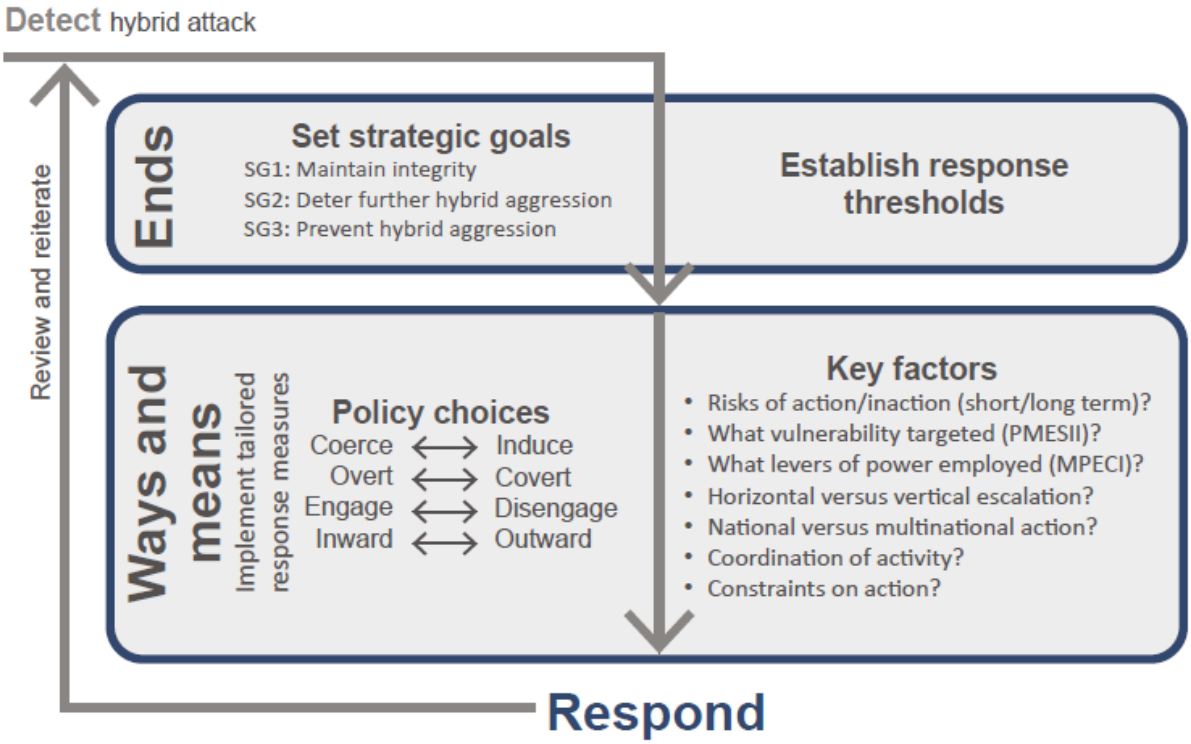

FIGURA 4 – Processo de resposta no combate à Guerra Híbrida[75]
Fonte: MCDC, 2019, p. 52.

Antes de mais nada, a decisão de responder a um ataque ou ameaça híbrida e como fazê-lo deve estar alinhada com o objetivo estratégico definido e apoiada em limites para resposta devidamente ajustados. A partir daí, segundo esse processo, a escolha das formas e meios que podem ser empregados deverá considerar certas opções de postura política[76] e fatores, identificados no estudo como fundamentais, além dos instrumentos do poder a serem usados (MCDC, 2019).

Essas opções de postura política são interdependentes e não mutuamente exclusivas, ou seja, elementos de cada uma delas poderão se unir para definir a postura que vai moldar o caráter de uma determinada resposta (MCDC, 2019). Elas envolvem os seguintes aspectos:

a) Engajar ou não — decidir até que ponto um ataque será reconhecido e confrontado. Expor uma atividade híbrida poderá melhorar a dissuasão, mas poderá legitimar a ação. Por outro lado, ignorá-la poderá impedir que ela volte a acontecer, uma vez que o inimigo ficará sem saber se o efeito desejado foi alcançado, mas poderá enfraquecer a capacidade de resposta da população (MCDC, 2019).

b) Agir interna ou externamente – definir se a resposta será voltada para o público

[75] Do original *The Countering Hybrid Warfare Response Framework* (tradução nossa).
[76] Do original *Policy choices* (tradução do autor).

interno ou externo (MCDC, 2019);

c) Ações ostensivas[77] ou sigilosas[78] – Essa definição dependerá da mensagem que se deseja transmitir com a ação, das reações que ela pode desencadear e de quem ela deve atingir (MCDC, 2019).

d) Coagir ou induzir – definir se a resposta será pautada em medidas assertivas para coagir o ator híbrido ou em medidas de estímulo para induzir o adversário a mudar seu comportamento (MCDC, 2019).

Todos esses aspectos mostram que a decisão de como responder a um ataque híbrido não deve ser tomada sem a devida consideração e deve ser fundamentada em informações as mais detalhadas possíveis sobre o agressor. Adicionalmente, ao avaliar essas opções, o modelo estudado propõe que os seguintes fatores devam ser levados em consideração na adoção de uma resposta:

– os riscos a curto, médio e longo prazo. Em particular, a possibilidade de uma escalada vertical do conflito em função de uma resposta (MCDC, 2019);

– as vulnerabilidades que serão alvo da resposta, sejam as do agressor ou as nossas, dependendo do foco das nossas ações (MCDC, 2019);

– quais instrumentos do poder serão empregados (MCDC, 2019);

– escalar a resposta horizontal e verticalmente, de modo a poder empregar respostas mais proporcionais, assimétricas e de fácil implementação (MCDC, 2019);

– se a resposta envolverá ações nacionais e/ou multinacionais (MCDC, 2019);

– a coordenação necessária para a resposta, tanto entre os setores do governo quanto com outros Estados (MCDC, 2019); e

– as restrições existentes, particularmente de ordem legal, para conferir legitimidade à resposta (MCDC, 2019).

Esses fatores servirão para moldar a resposta que será adotada. A questão de quais expressões do poder empregar e com que intensidade é fundamental para que a resposta dada seja eficaz em comunicar ao agente agressor que suas ações não serão toleradas, ao mesmo tempo em que passa segurança à sociedade e à comunidade internacional. Assim, veremos a seguir algumas considerações contidas no estudo do MCDC sobre as ações que podem ser adotadas nas diversas expressões do poder.

Assim como no caso da dissuasão, o estudo realizado pelo MCDC apresenta

[77] Consideradas no documento como aquelas que podem ser classificadas como públicas, óbvias e oficiais.
[78] Consideradas no documento como aquelas que podem ser classificadas como tendo uma audiência limitada, serem discretas e, até mesmo, negáveis.

exemplos e considerações sobre como as expressões do poder podem ser empregadas em resposta a ameaças híbridas. O APÊNDICE E – Ações para responder a ataques híbridos traz uma relação dessas medidas.

3.4.1 – A Resposta na Estratégia da União Europeia

Ao analisarmos a estratégia da UE no que tange à resposta a crises, verificamos que ela também traz uma abordagem bastante superficial desse aspecto, basicamente direcionada para o poder militar (COMISSÃO EUROPEIA 2016).

A estratégia europeia ressalta a importância de uma rápida resposta a ações desencadeadas por uma ameaça híbrida, do estabelecimento de um protocolo operacional comum entre os Estados Membros, em função do caráter multinacional da organização, da necessidade de coordenar as ações com a OTAN e da realização de exercícios nos diversos níveis para testar a capacidade de tomada de decisão (COMISSÃO EUROPEIA 2016).

É demonstrada, também, uma grande preocupação com o enquadramento legal de uma resposta a ataques híbridos (COMISSÃO EUROPEIA 2016). Isso se deve à necessidade de enquadrar o fato gerador da resposta nas cláusulas específicas de apoio mútuo da UE. Devido à natureza das atividades híbridas, torna-se difícil caracterizar a agressão, o que por vezes depende de uma questão de percepção. Assim, a UE vem estudando a aplicabilidade de algumas cláusulas específicas para a resposta a ataques híbridos.

Uma possível explicação para a falta de um maior detalhamento na abordagem de ações a serem implementadas em respostas a ataques híbridos pode estar em um estudo, também produzido para o MCDC, sobre o estado das políticas de combate à Guerra Híbrida (ARONSSON, 2019).[79] Nesse estudo, foi identificado que há um considerável desequilíbrio entre medidas ofensivas[80] e defensivas[81], como pode ser observado na FIG. 5, a seguir:

[79] O referido estudo analisou 18 publicações de governos, instituições e centros de estudos, que continham ao todo 110 ações de combate à Guerra Híbrida. Disponível em: <https://assets.publishing.service.gov.uk/ government/uploads/system/ uploads/attachment_data/file/803970/20190519-MCDC_CHW_Info_note_10-State_of_current_policy.pdf>.

[80] Geralmente relacionadas a respostas a ataques híbridos, aqui incluída a dissuasão por punição.

[81] Geralmente relacionadas com a dissuasão de agressores híbridos (principalmente por meio da negação, com medidas de resiliência, por exemplo).

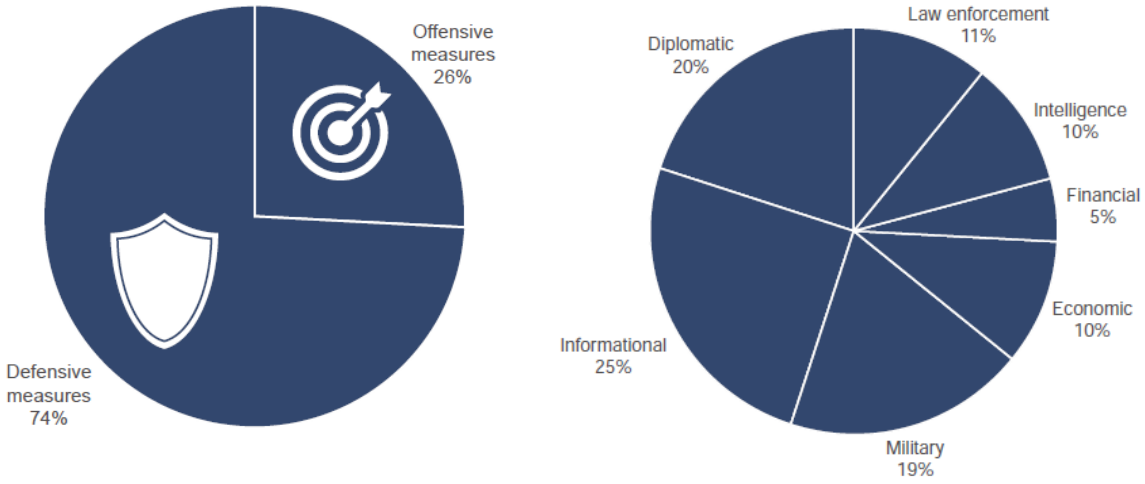

FIGURA 5 – Distribuição entre medidas ofensivas e defensivas de combate à Guerra Híbrida
Fonte: ARONSSON, 2019, p. 2.

Segundo esse estudo, alguns fatores podem explicar a preferência por medidas defensivas (ARONSSON, 2019):

a) Por ser um fenômeno ofensivo por natureza, a Guerra Híbrida tende a gerar respostas defensivas;

b) Os conceitos de resiliência e dissuasão são melhor desenvolvidos e compreendidos, o que lhes confere uma percepção de melhores chances de sucesso;

c) Muitas medidas defensivas têm custo menor e geram respostas mais previsíveis do que contramedidas assertivas; e

d) A comunidade internacional tende a julgar negativamente Estado que adotam medidas agressivas.

Os fatores apresentados acima trazem argumentos bastante lógicos para justificar a menor discussão sobre o emprego de medidas ofensivas no combate à Guerra Híbrida. Contudo, é importante que haja a compreensão no governo, na sociedade e no meio acadêmico de que tais medidas podem vir a ser necessárias e devem ser planejadas. Para isso, a realização de exercícios dentro de um cenário híbrido, com a participação de todos os setores do governo, ajudará a visualizar possíveis situações e a delinear eventuais respostas por todo o espectro das expressões do poder.

O referido estudo também identificou a natureza das ações propostas nas estratégias estudadas. Ao se analisar esse gráfico, observa-se que há um relativo equilíbrio entre as ações nos campos da informação, diplomático e militar. Tal fato pode estar relacionado com a natureza dos documentos estudados, mas também reflete a importância do domínio da informação nos conflitos modernos, em particular na Guerra Híbrida.

3.5 – Conclusões Parciais

Os atores do sistema internacional interagem entre si ao longo de uma larga faixa de atividades que vão desde a paz até o caso mais extremo de guerra ampla e irrestrita, passando por vários estágios graduados de acordo com sua intensidade e os meios envolvidos. Dentro desse *continuum*, a Guerra Híbrida, independentemente de ser um conceito novo ou não, é uma realidade dos conflitos atuais, em que forças convencionais e não convencionais são empregadas junto com as outras expressões do poder na consecução dos objetivos estabelecidos pelos atores.

Nesse contexto, a formulação de uma estratégica para combater a Guerra Híbrida é uma necessidade dos governos. Várias iniciativas vêm sendo desenvolvidas, principalmente na Europa, onde a sensação de insegurança é maior, em virtude dos recentes atos da Rússia na região.

De modo a apresentar uma base científica que possa orientar os governos na formulação de suas estratégias de combate à Guerra Híbrida, o MCDC(CHW) *Project* desenvolveu um modelo teórico estruturado em três componentes principais: detectar um ataque híbrido; dissuadir ataques híbridos; e responder a ataques híbridos. Esses três componentes devem ser orientados por objetivos estratégicos realistas e por limites para resposta bem definidos.

A detecção de ataques híbridos envolve o desenvolvimento de novos tipos de indicadores, o reposicionamento desses indicadores e a varredura do ambiente para identificar variações que, isoladamente, podem não trazer um significado específico, mas que, quando analisadas em conjunto com outras variações, proporcionam a percepção real da ameaça. Para isso, a criação de uma célula especializada mostrou-se uma solução adequada para a UE.

A dissuasão é um elemento fundamental em qualquer estratégia de combate à Guerra Híbrida, mas deve ser ajustada para fazer frente a escalada horizontal e vertical das ações híbridas. Ela deve estar baseada na resiliência da infraestrutura crítica e da sociedade. A realização de uma avaliação de riscos proporcionará um ponto de partida para as ações subsequentes.

Por fim, a resposta a ataques híbridos deve levar em consideração certos aspectos que ajudarão a definir a forma que a ação irá tomar. Em particular, devem ser visualizadas medidas empregando todas as expressões do poder.

Um estudo realizado apontou que a maioria das ações para combater a Guerra Híbrida estão inseridas no domínio da informação. Em particular, a desinformação tem se

mostrado uma ferramenta bastante utilizada por ameaças híbridas para levar a batalha para o domínio cognitivo. Dessa forma, dentro do escopo definido para este trabalho, passaremos a detalhar algumas estratégias específicas para o combate à desinformação.

4 O COMBATE À DESINFORMAÇÃO

"the time has come, when we all recognize, that words, camera, photo, the Internet and information in general have become yet another type of weapon, yet another type of armed forces." [82] (SHOYGU, 2015 *apud* EUROPEAN VALUES THIK TANK, 2016, p. 1).[83]

A livre circulação de ideias e o amplo debate são alguns dos alicerces que sustentam as sociedades democráticas (COMISSÃO EUROPEIA, 2018b). A internet permitiu que a circulação de ideias crescesse exponencialmente, aumentando o volume e a variedade das informações às quais as pessoas tem acesso e dando voz para que qualquer cidadão possa expressar suas opiniões. Contudo, essas mesmas características tornaram mais difícil avaliar a qualidade e a origem dessas informações, permitindo que a disseminação intencional de informações falsas ou, no mínimo, de informações empregadas fora do contexto possa ser intencionalmente usada para agravar divisões sociais, desacreditar instituições públicas ou privadas e criar uma narrativa tendenciosa de eventos. É o que, neste trabalho, consideraremos desinformação.

Nesse contexto, campanhas de desinformação podem ser empregadas por atores híbridos, valendo-se tanto da mídia tradicional quanto das novas plataformas, para radicalizar indivíduos ou grupos sociais, desestabilizar sociedades e controlar a narrativa política (COMISSÃO EUROPEIA, 2016). A negação e a distorção de fatos, junto com a intimidação, podem ser usadas para manipular a opinião pública e levá-la a questionar a legitimidade de eventuais respostas a ataques híbridos (RÂDULESCU, 2015).

Por esses motivos, uma estratégia para se contrapor à Guerra Híbrida deve possuir uma componente especificamente voltada para o combate à desinformação. Nesse sentido, descreveremos, a seguir, dois exemplos de iniciativas para fazer frente a ameaças dessa natureza: a estratégia de combate à desinformação adotada pela UE e a estratégia proposta pelo *European Values Center for Security Policy* para combater a desinformação. Com base na análise dessas duas iniciativas, buscaremos identificar ações que possam ser adotadas na elaboração de uma estratégia nacional de combate à desinformação.

---

[82] "Chegou a hora de todos reconhecermos que palavras, câmeras, fotos, a internet e a informação em geral se tornaram mais um tipo de arma, mais um tipo de Força Armada", tradução nossa.

[83] Sergey Shoygu, Ministro da Defesa russo desde 2012.

4.1 – A Estratégia da União Europeia para o Combate à Desinformação

As ações russas na crise da Ucrânia incentivaram a UE a adotar medidas para combater a desinformação e a transformaram em um elemento central na estratégia daquela organização para se contrapor a ameaças híbridas (FIOTT; PARKES, 2019). Para isso, em sua estratégia para combater ameaças híbridas, a UE orientou suas ações contra a desinformação em dois eixos: o primeiro eixo foi direcionado ao emprego da comunicação estratégica para fornecer respostas oportunas e baseadas em fatos e para aprimorar a conscientização da população quanto aos ataques sendo perpetrados pelos agressores híbridos; o segundo eixo focou no combate à disseminação de informações falsas, sem ferir os direitos fundamentais de liberdade de expressão e de acesso às informações (COMISSÃO EUROPEIA, 2016).

Essa estratégia foi sendo implantada gradativamente, por meio de iniciativas que foram desenvolvidas à medida que a questão da desinformação foi sendo estudada e o governo e a sociedade foram sendo mobilizados para enfrentá-la. A FIG. 6 apresenta uma visão geral dessas iniciativas, que serão abordadas a seguir:

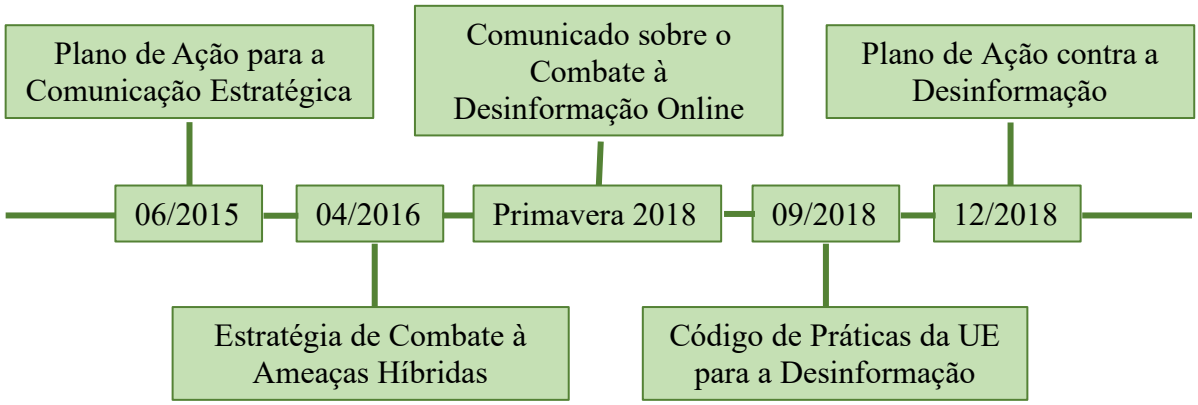

FIGURA 6 – Visão geral das ações da UE contra a desinformação[84]
Fonte: COMISSÃO EUROPEIA, 2019b, p. 1.

4.1.1 – O Plano de Ação para a Comunicação Estratégica

Inserido no primeiro eixo citado anteriormente, para refutar campanhas de desinformação, foi elaborado o Plano de Ação para a Comunicação Estratégica,[85] que previu a criação de equipes de Comunicação Estratégica como um primeiro passo nessa direção. Um

[84] Adaptada de figura encontrada em COMISSÃO EUROPEIA, 2019b, p.1.
[85] Do original *Action Plan on Strategic Communication*, tradução nossa. (HR/VP, 2015).

exemplo dessas equipes foi a *East StratCom Task Force*,[86] também conhecida como Caçadores de Mitos, [87] estabelecida para combater a desinformação russa (FIOTT; PARKES, 2019). Além da criação dessas equipes, esse plano de ação também priorizou o desenvolvimento de redes de comunicadores, jornalistas e representantes da mídia para amplificar o impacto e o alcance do material produzido, a realização de ações que promovessem a liberdade de imprensa e de expressão e o apoio à capacitação de jornalistas e profissionais da mídia (HR/VP, 2015). Outra importante área desse plano era o esforço a ser realizado para aumentar a conscientização do público em geral sobre a desinformação e promover um conhecimento mais aprofundado sobre a mídia (HR/VP, 2015).

A orientação das ações desse plano de ação deixa clara a importância do emprego das comunicações estratégicas contra a desinformação. Em um primeiro momento, elas têm uma grande participação na construção da resiliência da sociedade, transmitindo conhecimentos, combatendo divisões socais e fortalecendo as crenças e a confiança daquela população nas instituições do Estado. No caso da realização de uma campanha de desinformação ou de propaganda, que podem ser parte de uma campanha híbrida mais ampla, as comunicações estratégicas serão uma ferramenta fundamental para o controle da narrativa.

Após o estabelecimento das ações no campo das comunicações estratégicas e aderente aos eixos estabelecidos em sua estratégia para combater ameaças híbridas, a UE passou a desenvolver ações no sentido de melhorar a qualidade das informações que são disseminadas pelos meios de comunicação. Assim, em 2018, três iniciativas foram adotadas pela UE, junto com os Estados Membros e plataformas online. Essas iniciativas serão apresentadas a seguir.

4.1.2 – Comunicado sobre o Combate à Desinformação Online: uma Abordagem Europeia[88]

A primeira dessas iniciativas deu-se por meio de um comunicado da Comissão Europeia (COMISSÃO EUROPEIA, 2018b) que reconheceu a desinformação como uma ferramenta da Guerra Híbrida e o papel desempenhado pela sociedade e pelo setor privado no combate à essa ameaça (COMISSÃO EUROPEIA, 2018d). Com base nesses aspectos, foram delineados princípios e objetivos gerais e estabelecidas medidas para aumentar a conscientização do público e combater a desinformação (COMISSÃO EUROPEIA, 2018b). A estratégia proposta foi baseada em quatro princípios: melhorar a transparência sobre a origem

[86] Força-Tarefa de Comunicação Estratégica Leste, tradução nossa.
[87] Do original: *Myth Busters*, tradução nossa (JOPLING, 2018).
[88] Do original Communication on Tackling online desinformation: a European Approach, tradução nossa (COMISSÃO EUROPEIA, 2018b).

das informações e como elas são produzidas, patrocinadas e disseminadas; promover a diversidade da informação, apoiando o jornalismo de alta qualidade e a educação sobre a mídia;[89] incentivar a credibilidade das informações, indicando sua confiabilidade, facilitando sua rastreabilidade e a autenticação das fontes; e criar soluções inclusivas baseadas na cooperação de todas as partes envolvidas (COMISSÃO EUROPEIA, 2018b).

As ações contidas nesse documento focaram na construção de um ambiente midiático menos suscetível à desinformação. Para isso, além de adotar ações para melhorar a capacitação dos profissionais do setor e a compreensão da população como um todo sobre a dinâmica da desinformação, essa diretriz demonstra uma grande preocupação em mobilizar o setor privado para que este assuma suas responsabilidades na garantia da qualidade e na transparência das informações a que seus usuários estão tendo acesso. Esse esforço resultou na formulação de um compromisso assumido pelas principais plataformas online para auxiliar no combate à desinformação, como será mostrado a seguir.

4.1.3 – O Código de Práticas da UE para a Desinformação

A segunda iniciativa para melhoria da qualidade das informações foi a adoção do Código de Práticas da EU para a desinformação[90] pelas principais plataformas online, como Facebook, Google, Twitter, Mozilla e, posteriormente, Microsoft. Essas plataformas e seus anunciantes, de maneira voluntária, reconheceram seu papel e suas responsabilidades no processo de combate à desinformação e concordaram em adotar parâmetros para auto regulação (COMISSÃO EUROPEIA, 2018b). Segundo Fiott e Parks (2019), a opção pela auto regulação foi decorrente do desafio de garantir o cumprimento, pelas empresas de mídia, de uma regulamentação impositiva sobre o assunto. Como essas empresas já vinham tendo que cumprir obrigações legais para combater e dissuadir discursos de ódio, discriminação racial e de gênero, esses autores entendem que a auto regulação seria uma solução de equilíbrio entre a abertura e a regulamentação (FIOTT; PARKES, 2019).

Esse Código de Práticas foi centrado em onze esforços principais, entre os quais ressalta-se (COMISSÃO EUROPEIA, 2018c):

a) A criação de salvaguardas contra a desinformação;

b) A redução das receitas de propagandas que contenham desinformação;

c) A garantia da transparência da propaganda política ou daquela baseada em

[89] Referente ao termo original em inglês “media literacy”, que pode ser traduzido como alfabetização midiática.
[90] Do original *EU Code of Practise on Disinformation*, tradução nossa. (COMISSÃO EUROPEIA, 2018c).

questões em discussão na sociedade;

d) O fechamento de contas falsas e a regulação do uso de robôs para distribuição de mensagens;

e) O investimento em tecnologias para promover conteúdo confiável; e

f) A flexibilização do acesso a dados para verificação das informações e das atividades de pesquisa, em conformidade com as políticas de privacidade.

Além dessas ações, o Código de Práticas também traz uma relação de boas condutas que os signatários adotarão para implementá-lo e prevê relatórios anuais para informar sobre o andamento e resultado das medidas adotadas. Ao se comprometerem com a fiscalização da veracidade e transparência do conteúdo de suas plataformas, essas empresas, além de cultivarem a confiança dos usuários no ambiente midiático, também auxiliarão na detecção e análise de informações falsas, o que pode ter um grande efeito contra a desinformação.

Obviamente, como se trata de uma autorregulação, não há uma padronização nos critérios dessa fiscalização, ficando a cargo de cada uma delas definir o que se enquadra como desinformação. Daí a importância, também, da participação de pessoas e instituições voltadas para a verificação dos fatos. Para que essa participação seja possível, é importante o acesso aos dados das plataformas, respeitadas as políticas de proteção de dados.

Por fim, esse Código de Práticas contribuirá para a resposta a ataques híbridos, pois as plataformas online se comprometeram a adotar sanções contra as fontes da desinformação, como a retirada de conteúdo falso, o encerramento de contas e perfis falsos e a redução dos ganhos com propaganda. Embora, mais uma vez, essas ações sejam dependentes dos critérios estabelecidos por cada plataforma, elas representam um passo significativo em direção a um ambiente midiático mais seguro. Faltava, agora, um plano para orientar as ações dos diversos setores da UE e dos Estados Membros.

4.1.4 – O Plano de Ação contra a Desinformação

Por último, a UE formulou o Plano de Ação contra a Desinformação,[91] com medidas adicionais e concretas para proteger o sistema democrático europeu e combater a desinformação. Para isso, a UE estabeleceu ações para aumentar a capacidade de expor as atividades de desinformação, melhorar a coordenação de respostas entre os diversos setores e os Estados Membros, cobrar das plataformas online o cumprimento do código de conduta e

[91] Do original *Action Plan Against Disinformation*, tradução nossa (COMISSÃO EUROPEIA, 2018a).

aumentar a conscientização e a participação da sociedade (COMISSÃO EUROPEIA, 2018c). Serão identificadas, abaixo, as principais ações em cada uma dessas áreas.

Para melhorar a capacidade de detectar, analisar e expor a desinformação, o plano de ação previu o reforço da estrutura e dos meios das *Strategic Communication Task Forces* e da *EU Hybrid Fusion Cell*. O reforço de pessoal incluiria peritos em processos de mineração e análise de dados e em idiomas. Adicionalmente, investimentos em sistemas de TI foram feitos para facilitar a análise de grandes volumes de dados (COMISSÃO EUROPEIA, 2018c).

A criação de um Sistema de Alerta Rápido[92] foi a medida adotada para melhorar a capacidade de coordenar respostas oportunas a ataques híbridos. Ele é organizado em torno de uma plataforma digital dedicada e envolve a participação de vinte e oito pontos de contato nacionais, além de setores dentro da UE. Com esse sistema, a UE buscou facilitar o compartilhamento de dados e avaliações sobre campanhas de desinformação e prover alertas em tempo real sobre ameaças dessa natureza. Assim, espera-se alcançar maior eficácia na elaboração de respostas proativas e objetivas à desinformação, com foco nos valores e políticas conduzidas (COMISSÃO EUROPEIA, 2018a).

No que tange às plataformas online, aos anunciantes e ao setor de publicidade, o plano de ação reconheceu, novamente, a importância da participação dessas entidades no combate à desinformação e reforçou a necessidade de que elas cumpram o acordado no código de conduta (COMISSÃO EUROPEIA, 2018a). A UE previu o monitoramento da implementação das ações para poder cobrar as empresas envolvidas e avaliar a eficácia do código e os ajustes necessários, inclusive de natureza regulatória (COMISSÃO EUROPEIA, 2018a).

Como último pilar do plano de ação, a UE reforçou as ações já estabelecidas no Plano de Ação para a Comunicação Estratégica, no sentido de melhorar a conscientização do público, proporcionando "uma melhor compreensão sobre as fontes de desinformação e sobre as intenções, ferramentas e objetivos por trás da desinformação, mas também de nossas próprias vulnerabilidades" (EUROPEAN COMMISSION, 2018a, p.9). Para isso, a UE previu a organização de campanhas direcionadas para educar a população sobre a mídia e treinamento para profissionais da área e formadores de opinião (COMISSÃO EUROPEIA, 2018a). Buscou, também, apoiar o trabalho da mídia independente e o jornalismo de qualidade e desenvolver redes independente de pesquisadores e de pessoas interessadas em contribuir para a verificação de fatos (COMISSÃO EUROPEIA, 2018a).

---

[92] Do original *Rapid Alert System*, tradução do autor. Maiores detalhes em: <https://eeas.europa.eu/sites/eeas/files/ras_factsheet_march_2019_0.pdf.

O Plano de Ação contra a Desinformação completou as iniciativas da UE para enfrentar o problema da desinformação. As ações e determinações contidas nele têm o potencial para melhorar a forma com que os Estados membros e a própria UE lidam com o problema, proporcionando uma abordagem que engloba a detecção e análise de eventuais atos de desinformação, o fortalecimento da sociedade e das instituições contra essas ações e a coordenação de respostas oportunas, seja pelo emprego de comunicações estratégicas, seja atuando junto às plataformas online.

Embora os documentos estudados até agora neste capítulo apresentem objetivos bem definidos que orientam as ações adotadas, ao analisarmos a estratégia como um todo verificamos que a definição dos seus objetivos não fica clara. Isso pode ser decorrente da falta de um documento mais amplo, que estabeleça os eixos estruturantes dessa estratégia e o contexto de cada um desses documentos específicos dentro dela.

Apesar de a estratégia como um todo ser bastante abrangente e bem direcionada às fragilidades exploradas pela desinformação, sua eficácia dependerá, em grande parte, de sua implementação, particularmente por depender das ações dos Estados Membros. Como o ambiente de segurança europeu está bastante sensível ao tema, percebe-se o comprometimento de todos os envolvidos, Comissão Europeia, Estados Membros, setor privado, instituições civis e sociedade, com o combate à desinformação, o que se reflete nos resultados alcançados como poderá ser visto a seguir.

4.1.5 – Andamento das Ações e Resultados Alcançados

Em um relatório publicado em junho de 2019 (COMISSÃO EUROPEIA, 2019b), a UE divulgou as ações que vêm sendo realizadas em atendimento às iniciativas citadas neste capítulo e apresentou alguns resultados obtidos com suas ações contra a desinformação.

Segundo esse relatório, a UE vem ampliando a capacidade da *East Stratcom Task Force*, que atuou contra mil ações de desinformação entre janeiro e junho de 2019, em comparação com 434 casos no mesmo período de 2018 (COMISSÃO EUROPEIA, 2019b). O Sistema de Alerta Rápido foi estabelecido em março de 2019 e tem conseguido aumentar o número de interações entre os setores da UE e pontos de contato nacionais dos Estados Membros, por meio de uma plataforma digital dedicada (COMISSÃO EUROPEIA, 2019b).

Sobre o Código de Conduta, o relatório traz números bastante significativos sobre a atuação das plataformas digitais, como 2,2 milhões de contas falsas canceladas pelo Facebook e 3,39 milhões de canais removidos pelo Youtube (COMISSÃO EUROPEIA, 2019b).

Por último, foram apresentadas ações adotadas direcionadas à melhoria da conscientização e da resiliência (COMISSÃO EUROPEIA, 2019b), como a Semana Europeia da Educação sobre a Mídia[93] e três campanhas conduzidas sobre a desinformação, com potencial para alcançar 240 milhões de contatos.[94]

Ao que tudo indica, dentro do contexto da UE, as medidas adotadas de acordo com a estratégia estabelecida para combater a desinformação têm se mostrado ferramentas apropriadas para esse fim. O que não quer dizer que a batalha esteja sendo ganha, uma vez que o volume de informações e fontes disponíveis na mídia, principalmente online, tornam complicado identificar e rebater todas as atividades de desinformação antes que elas possam causar algum tipo de dano.

Além disso, é de se esperar que atores interessados em fazer uso da desinformação não fiquem inertes diante dessas iniciativas e busquem formas de se contraporem às ações da estratégia da UE. É interessante, então, identificar outras abordagens para enfrentar a desinformação e enriquecer o estudo desse assunto. Assim, será apresentada a estratégia proposta por uma outra instituição europeia para lidar com a ameaça da desinformação.

4.2 – A Estratégia do *European Values Center for Security Policy*

O *European Values Center for Security Policy* é um instituto não governamental que tem como objetivo contribuir para a defesa da República Tcheca e da Europa como um todo melhorando a cultura política de seus cidadãos.[95] De acordo com os dados mais recentes disponíveis, esse centro de estudos é financiado por várias instituições, entre elas o governo da Holanda, do Reino Unido, dos EUA, de Israel, da Ucrânia e da Comissão Europeia.[96] Um dos seus principais programas é o *Kremlin Watch*, que procura combater os instrumentos de influência e as operações de desinformação russas.

Em um documento de 2016 (EUROPEAN VALUES THINK TANK, 2016), esse instituto de pesquisa propôs uma estratégia de combate à desinformação estruturada em quatro eixos ou áreas de resposta. Essa estratégia foi orientada para a situação específica da República Tcheca e da UE, diante da percepção de uma ameaça russa. Por isso, as medidas propostas incluem ações a serem adotadas pelos governos nacionais, pelos organismos multinacionais,

---

[93] Do original *European Media Literacy Week*, tradução nossa.
[94] Invest EU, #EUandMe e EU Protects.
[95] Conforme apresentado no site da instituição. Disponível em: <https://www.europeanvalues.net/o-nas/nase-poslani/>.
[96] De acordo com seu relatório anual, disponível em: <https://www.europeanvalues.net/wp-content/uploads/2019/10/Annual-Report-2018.pdf>.

como a UE e a OTAN, e pela sociedade direcionadas contra as ações da Rússia na região. Porém, muitas das medidas propostas podem ser adaptadas para serem empregadas em outros contextos. Detalharemos a seguir cada um dos quatro eixos da estratégia proposta e suas principais ações.

4.2.1 – Inclusão da Questão da Desinformação na Agenda da Política Externa e da Segurança

Por considerar que uma ameaça só poderá ser combatida quando for reconhecida e compreendida pelo governo e for inserida em suas políticas públicas, o primeiro eixo da estratégia envolveu ações direcionadas à inclusão do problema da desinformação na agenda da política externa e da segurança (EUROPEAN VALUES THINK TANK, 2016). Assim, essa estratégia propõe que os governos nacionais definam as campanhas de desinformação russas como uma ameaça à segurança nacional e incluam-na em suas estratégias de segurança e de política externa (EUROPEAN VALUES THINK TANK, 2016). Ressaltam-se, ainda, três outras medidas contidas nesse eixo:

a) O monitoramento e a exposição de ligações entre o governo russo e grupos extremistas, que tanto podem ser alvos da desinformação, agravando divisões sociais no país, quanto podem ser ferramentas para a disseminação da desinformação (EUROPEAN VALUES THINK TANK, 2016);

b) A criação de unidades financeiras de ação rápida,[97] que tenham a capacidade para, rapidamente, congelar ou, até mesmo, confiscar bens de Estados, organizações e indivíduos em retaliação a campanhas de desinformação (EUROPEAN VALUES THINK TANK, 2016). De acordo com Edward Lucas (2018), essas ações requerem um elevado grau de coordenação entre instituições, por vezes de mais de um país, e que, por isso, a realização de exercícios periódicos é recomendada para identificação e solução de obstáculos. Ainda segundo esse autor, essas unidades devem envolver representantes da área de inteligência, do setor financeiro e do poder judiciário, com autoridade para tomar as decisões e realizar os contatos necessários; e

c) Deverá ser buscada maior aproximação com o Centro de Excelência para Comunicação Estratégica da OTAN, por meio da realização de exercícios conjuntos e treinamentos (EUROPEAN VALUES THINK TANK, 2016).

---

[97] Do original *Financial Snap Unit*, tradução nossa.

4.2.2 – Questionar Publicamente os Apoiadores da Desinformação Patrocinada pela Rússia

O segundo eixo da estratégia foca no enfraquecimento do apoio interno às ações de desinformação russas. Para isso, representantes dos interesses russos, principalmente políticos e figuras públicas, devem ter esse vínculo exposto publicamente, para permitir às pessoas compreender as motivações por trás de suas ações (EUROPEAN VALUES THINK TANK, 2016).

Nesse sentido, essa estratégia propõe, dentre outras medidas, que os governos investiguem as finanças e as ligações de políticos com o governo russo, atuem para que esses políticos não assumam cargos relacionados à área de inteligência ou da segurança nacional e garantam a transparência do financiamento de partidos políticos (EUROPEAN VALUES THINK TANK, 2016).

Além disso, também é proposto que representantes da sociedade, como ONG, institutos de pesquisa e jornalistas participem desse esforço. Essa participação estaria centrada na investigação, na divulgação e na exposição pública das pessoas e organizações envolvidas com a desinformação. Tais ações deveriam ser complementadas por uma mobilização para que seus autores prestem contas de suas ações e da origem de seus recursos (EUROPEAN VALUES THINK TANK, 2016).

4.2.3 – Divulgar o Conteúdo e os Veículos de Campanhas de Desinformação

O terceiro eixo propõe medidas para expor o conteúdo e os veículos empregados em campanhas de desinformação (EUROPEAN VALUES THINK TANK, 2016). Atualmente, a grande quantidade de canais de comunicação, principalmente na internet, dificulta a identificação dos canais que realmente dispõem de um conteúdo sério e daqueles que simplesmente publicam opiniões pessoais de fatos, informações infundadas ou meramente falsas. É necessário identificar as notícias falsas, questioná-las publicamente com base em fatos e responsabilizar seus canais de divulgação, de modo a desacreditá-los perante a sociedade, enfraquecendo sua influência negativa (EUROPEAN VALUES THINK TANK, 2016).

O primeiro passo proposto nessa direção é a criação de equipes nacionais de análise da desinformação,[98] para monitorar a mídia, identificar ações de desinformação e preparar e coordenar respostas (EUROPEAN VALUES THINK TANK, 2016). Apesar de se tratar de uma

[98] Do original *National Disinformation Analysis Teams*, tradução nossa.

atividade de inteligência, o foco do trabalho não deve ser militar, mas um conjugado multidisciplinar de capacidades para que se possa identificar a ameaça, avaliar seu potencial de dano e acionar os setores adequados do governo e da sociedade envolvidos na resposta (EUROPEAN VALUES THINK TANK, 2016). Tais equipes também devem estabelecer relações de confiança com canais de comunicação sérios, para agilizar e potencializar essas respostas (EUROPEAN VALUES THINK TANK, 2016).

Duas outras medidas propõem a revisão do arcabouço legal. Muitas leis e normas relativas à liberdade de expressão, à livre circulação de ideias, à proteção a dados pessoais e corporativos, à concessão de transmissão de rádio e televisão e às responsabilidades de plataformas online foram estabelecidas em um contexto diferente do atual, em que as ameaças de mal uso da informação não eram tão presentes ou tão abrangentes. Dessa forma, essa revisão deve buscar identificar as brechas existentes que facilitem a realização de campanhas de desinformação e prever medidas para responsabilizar e punir quem as perpetrarem (EUROPEAN VALUES THINK TANK, 2016).

Por fim, ainda dentro de um contexto de combate ao conteúdo e aos meios de divulgação da desinformação, prevê ações a serem conduzidas pelas instituições civis. Dentre elas, o incentivo, apoio e até financiamento de ONG, instituições e iniciativas individuais que busquem identificar e desconstituir narrativas falsas (EUROPEAN VALUES THINK TANK, 2016). Por não estarem limitados pela burocracia do governo, esses atores têm capacidade de mais rapidamente agirem contra a desinformação e, por estarem inseridos na sociedade, podem conferir maior credibilidade a esse esforço. Em particular, a estratégia do *European Values Think Tank* estabelece que as associações de jornalistas devam participar ativamente dessas atividades, educando os profissionais e o público sobre a questão, fiscalizando a conduta ética de seus associados e, quando pertinente, aplicando seus códigos de conduta contra aqueles que se valem de uma pretensa atividade jornalística para ações de desinformação (EUROPEAN VALUES THINK TANK, 2016).

4.2.4 – Construir a Resiliência da Sociedade

O último eixo dessa estratégia é direcionado a ações para reforçar a resiliência das sociedades contra a desinformação (EUROPEAN VALUES THINK TANK, 2016). Como já visto anteriormente, as sociedades precisam estar preparadas para lidar com ataques híbridos, em particular aqueles direcionados domínio cognitivo da população, aos seus valores fundamentais e instituições e ao seu tecido social. O primeiro passo proposto nessa direção é

uma avaliação detalhada e regular das tensões e insatisfações dentro da sociedade, que possam ser exploradas em uma campanha de desinformação (EUROPEAN VALUES THINK TANK, 2016). Com base nessas avaliações, o Estado poderá definir medidas específicas para lidar com essas questões. Essas medidas podem incluir o uso de emissoras públicas para realizar campanhas de conscientização e educação da população sobre a desinformação e a formulação de políticas de inclusão de minorias, particularmente as de origem russa, proporcionando acesso a mídias independentes em suas línguas de origem (EUROPEAN VALUES THINK TANK, 2016).

Um aspecto importante se refere à resiliência dentro das Forças Armadas e das forças de segurança internas (EUROPEAN VALUES THINK TANK, 2016). Campanhas de desinformação podem ser empregadas para enfraquecer as lideranças militares perante suas tropas, a credibilidade das forças de segurança junto à população e a confiança das tropas em sua capacidade de combater o agressor. Assim, o monitoramento de esforços nesse sentido por eventuais agressores, o acompanhamento constante do moral da tropa, por meio de pesquisas internas, e o esforço regular de educação sobre a desinformação são medidas que devem ser adotadas (EUROPEAN VALUES THINK TANK, 2016). Além disso, as lideranças militares devem fazer uso intenso das comunicações estratégicas para reforçar os valores das instituições e garantir que as ações tomadas no mais alto nível sejam compreendidas até mesmo nos escalões mais baixos, não dando margem para interpretações maliciosas que possam ser exploradas por agressores híbridos.

As últimas medidas nesse eixo envolvem a qualificação de profissionais para atuarem no campo das comunicações estratégicas e o ensino de um conteúdo relacionado à desinformação nos cursos de formação de jornalismo (EUROPEAN VALUES THINK TANK, 2016). A primeira medida visa a atender uma demanda específica de profissionais de comunicação com "conhecimento das leis, relações internacionais, políticas de segurança, assuntos de defesa, ambiente da mídia, mídias sociais e realidades da ciência política" (EUROPEAN VALUES, 2016, p 23). Ao mesmo tempo, a estratégia considera que os jornalistas tem a responsabilidade perante a sociedade de garantir a transparência e a confiabilidade do ambiente das informações. Para isso, a inserção de conhecimentos sobre o modus operandi da desinformação nos cursos das faculdades irá colocar no mercado profissionais melhores preparados para identificar e lidar com essa questão (EUROPEAN VALUES THINK TANK, 2016).

Assim como a estratégia da UE, as medidas propostas pelo *European Values Think Tank* envolvem uma ampla gama de atividades e requerem a participação de diversos setores

do governo e da sociedade. Algumas dessas medidas se aproximam muito daquelas encontradas na estratégia da UE, como as relacionadas à identificação e análise de informações falsas, à transparência e confiabilidade das informações, à participação da sociedade, em particular dos profissionais e empresas da área, no combate à desinformação e à melhoria da resiliência.

Por outro lado, algumas medidas trouxeram uma abordagem diferente para o problema, como a revisão do arcabouço legal, a preocupação em identificar os focos de tensão da sociedade que podem ser explorados pela desinformação e o combate aos aspectos financeiro e político da desinformação. Tanto as similaridades quanto as divergências das duas estratégias enriqueceram essa análise comparativa e permitiram identificar objetivos e ações a serem adotados pelo Brasil para combater a desinformação.

4.3 – Uma Proposta de Estratégia de Combate à Desinformação

Revendo os conceitos sobre a desinformação, explorados no capítulo dois, depreende-se que ela explora vulnerabilidades existentes dentro dos Estados, tanto no governo quanto na sociedade, para enfraquecer sua coesão social e política e atuar sobre o domínio cognitivo daquele ambiente. Para isso, um ator hostil faz uso da rápida e ampla disseminação de informações falsa ou manipuladas, de modo a conquistar e manter o controle da narrativa de uma situação específica. Ele se aproveita de um ambiente midiático vulnerável, intenso e difuso, em que os esforços para verificação de fatos, quando existem, são descoordenados.

Ainda que esse ator hostil consiga agir, ele só terá êxito em suas ações se encontrar as condições favoráveis para que essa desinformação dê resultados. Essas condições envolvem uma sociedade incapaz de avaliar o conteúdo, a origem e o propósito por trás dessas ações, uma mídia local despreparada para lidar com o problema e um governo que não consiga acompanhar a evolução da situação, estabelecer o controle da narrativa e mobilizar todos os setores da sociedade para combater essas ações.

Assim, tomando como referência o modelo proposto pelo MCDC(CHW) *Project* para o combate à Guerra Híbrida e com base nos exemplos estudados acima, é possível formular uma estratégia de combate à desinformação, conforme o QUADRO 1, a seguir:

QUADRO 1

Estratégia proposta para combater a desinformação

OBJETIVO		MODELO DO MCDC
Objetivo 1 – Desenvolver a capacidade de detectar, analisar e expor a desinformação		
AÇÃO	Estabelecer um órgão para detecção e análise da desinformação.	Detectar
	Identificar e monitorar vínculos entre atores hostis e grupos extremistas, pessoas públicas e organizações midiáticas.	Detectar
	Desenvolver junto com os setores do governo, os estados e a sociedade um sistema de alerta de desinformação.	Detectar
Objetivo 2 – Empregar a comunicação estratégica de maneira eficaz.		
AÇÃO	Estabelecer um órgão vocacionado para a comunicação estratégica.	Dissuadir e responder
	Estabelecer, junto à sociedade, uma rede de apoio à comunicação estratégica.	Dissuadir e responder
Objetivo 3 – Mobilizar o setor privado		
AÇÃO	Desenvolver, junto às empresas do setor de mídia, mecanismos para assegurar a transparência e credibilidade das informações e a rastreabilidade de suas origens.	Detectar e Dissuadir
	Desenvolver, junto às empresas do setor de mídia, mecanismos para promover a prestação de contas de quem contribuir para a desinformação.	Responder
Objetivo 4 – Fortalecer o ambiente midiático		
AÇÃO	Garantir a liberdade de expressão e de imprensa.	Dissuadir
	Melhorar a capacitação de jornalistas e de atores da mídia.	Dissuadir
	Apoiar o jornalismo de qualidade.	Dissuadir
	Fortalecer a capacidade de verificação de fatos da sociedade.	Dissuadir
	Educar a mídia sobre a desinformação.	Dissuadir
Objetivo 5 – Desenvolver a resiliência		
AÇÃO	Promover a educação digital e midiática da sociedade.	Dissuadir
	Aumentar a conscientização sobre a desinformação.	Dissuadir
	Revisão do arcabouço legal para facilitar a detecção e resposta à desinformação.	Dissuadir
	Fortalecer a liderança, o moral e a disciplina nas forças de segurança, em particular nas Forças Armadas, realizando o acompanhamento constante do ambiente interno dessas instituições.	Dissuadir
	Realizar avaliações detalhadas e regulares de tensões, polarizações e insatisfações dentro da sociedade.	Dissuadir

Fonte: Quadro elaborado por este autor.

Os objetivos estabelecidos na estratégia proposta buscam atuar sobre cada um dos aspectos abordados anteriormente neste subitem, reduzindo as vulnerabilidades que potencializam o resultado de ações de desinformação. Já as ações estabelecidas, formuladas com base nos exemplos estudados, são uma solução inicial para o problema. Outras necessidades poderão surgir, dependendo das condições específicas a serem enfrentadas, como no caso da Ucrânia, onde o ambiente midiático era fortemente influenciado pela mídia de

origem russa, que tinha grande influência sobre certos grupos na região

4.4 – Conclusões Parciais

As estratégias abordadas neste capítulo, apesar de formuladas para o contexto multinacional específico da Europa, proporcionaram *insights* bastante interessantes que serviram de base para a formulação de uma estratégia que possa ser adotada pelo Brasil para combater a desinformação. Porém, é importante considerar que uma campanha de desinformação pode estar inserida dentro de um contexto mais amplo de emprego de uma estratégia híbrida. É fundamental, então, que medidas de combate à desinformação estejam inseridas, também, dentro de uma estratégia mais ampla de combate à Guerra Híbrida.

Mesmo com uma estratégia bem estruturada e definida, as dificuldades para o combate à desinformação são grandes. Primeiro, pelo grande volume de informações e fontes existente hoje em dia e com tendência de aumentar ainda mais, o que dificulta sua identificação e análise. Segundo, pelo importante papel de atores privados nesse processo, sejam eles plataformas de mídia social, influenciadores ou grandes empresas da mídia tradicional, cujos interesses nem sempre estão alinhados com os do Estado. Terceiro, pela dificuldade de regulamentar as plataformas online e as restrições de acesso aos dados de modo a dar maior transparência às informações, e, por último, a dimensão do esforço para aprimorar o conhecimento da sociedade sobre a mídia.

Mesmo assim, apesar dessas dificuldades, é de extrema importância que os Estados estejam preparados para lidar com essa ameaça. Para isso, uma sólida estratégia de combate à desinformação é primordial. Assim, de modo a avaliarmos a eficácia da estratégia proposta, faremos a análise das ações nela contidas, à luz das ações de desinformação empregadas na campanha híbrida da Rússia contra a Ucrânia.

5 ANÁLISE DA ESTRATÉGIA PROPOSTA

Para avaliarmos a pertinência da estratégia proposta no combate à desinformação, identificaremos, neste capítulo, as principais características da campanha de desinformação empregada pela Rússia contra a Ucrânia, dentro do espectro mais amplo do que foi caracterizado como uma Guerra Híbrida.

Em seguida, vamos analisar se objetivos e ações propostos conseguiriam minimizar as vulnerabilidades apresentadas pela Ucrânia, que tornaram possíveis as ações russas, ou se elas conseguiriam atenuar os efeitos das próprias ações russas. Com isso, esperamos concluir se a estratégia proposta poderia ser adotada como uma base para o desenvolvimento uma estratégia nacional para combater a desinformação no contexto da Guerra Híbrida.

5.1 A Campanha de Desinformação Russa na Ucrânia em 2014

"The most amazing information warfare blitzkrieg we have ever seen in the history of information warfare." [99] (General Philip Breedlove, 2014).[100]

Nesta sua formação mais recente, após o fim da União Soviética, a Ucrânia apresenta uma divisão cultural bastante nítida. Sua porção ocidental tem uma orientação voltada para a Europa e o Ocidente, enquanto suas porções oriental e Sul tem laços étnicos e culturais com a Rússia (SAZONOV *et al*, 2016). Um grande exemplo disso era o grau de penetração da mídia russa nessas regiões até 2014, onde as redes de rádio e televisão e os jornais, além dos sites de notícias, eram, em sua maioria, de origem russa (KOFMAN *et al*, 2017). Mesmo os programas de televisão dos canais ucranianos transmitiam programação produzida na Rússia (KOFMAN *et al*, 2017).

Durante o governo do ex-presidente Viktor Yanukovych, um político pró-Rússia, a Ucrânia vinha negociando um acordo de associação com a UE. Contudo, no final de 2013, diante da decisão do governo de não mais assinar esse acordo, começaram a ocorrer manifestações populares contrárias a essa decisão. Essas manifestações e as respostas do governo foram se tornando mais violentas, até que, em 22 de fevereiro de 2014, Yanukovych foi retirado do poder e substituído por uma coalizão pró-Ocidente.[101] Ele e boa parte da elite governante fugiram para a Rússia e um governo interino foi estabelecido (KOFMAN *et al*,

[99] "A mais incrível blitzkrieg de guerra de informação que nós já vimos na história da guerra de informação", tradução nossa.
[100] Comandante Supremo Aliado da OTAN, se referindo à guerra de informação russa contra a Ucrânia em 2014. Disponível em: < https://www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464>.
[101] No que ficou conhecido como a Revolução Maidan (nome da praça central de Kiev) ou Euromaidan.

2017).

Com a queda de Yanukovych, o governo de Kiev voltou a buscar a integração com o Ocidente. Para Moscou, esses dois fatos representavam a grande ameaça de ter a Ucrânia retirada de sua esfera de influência (KOFMAN *et al*, 2017), além de colocar a UE e a OTAN em suas fronteiras. Além disso, a Rússia possui uma base naval em Sebastopol, na Crimeia, que lhe dá acesso às águas quentes do Mar Negro e é de fundamental importância estratégica.

Para se opor a essa situação e manter o controle sobre, pelo menos, parte do território da Ucrânia, a Rússia invadiu e ocupou a Criméia em março de 2014 (SAZONOV *et al*, 2016). Simultaneamente, o governo de Putin fomentou dissenções no Leste do país, que se transformaram, em pouco tempo, em uma violenta insurgência (KOFMAN *et al*, 2017). Com o apoio já não tão velado da Rússia, o conflito cresceu em proporção, sem que nenhum dos lados conseguisse se impor, até que, após elevadas mortes, as partes acordaram um cessar fogo em setembro de 2014 (KOFMAN *et al*, 2017). Desde então, a situação permanece instável na região, com diversos cessar-fogo posteriores ao primeiro, sem que haja uma solução definitiva para a questão.

As ações da Rússia nesse conflito se tornaram o paradigma da Guerra Híbrida (PINHO, 2016). O governo russo procurou explorar as vulnerabilidades políticas, econômicas e, principalmente, psicossociais da Ucrânia. Para isso, as atividades militares foram fortemente apoiadas por uma campanha ativa na mídia (SAZONOV *et al*, 2016), em um esforço para controlar o fluxo de informações (JAITNER, 2015).

Assim, a Guerra de Informação russa tornou-se um componente crítico da sua Guerra Híbrida, com base no conceito de controle reflexivo,[102] sendo empregada na Ucrânia desde o nível político até o nível tático militar (SAZONOV *et al*, 2016). Segundo Snegovaya (2015, p. 9, tradução nossa), a Guerra de Informação russa "consiste de uma campanha deliberada de desinformação apoiada por ações dos órgãos de inteligência destinadas a confundir o inimigo e obter vantagem estratégica a um custo mínimo". Por exemplo, ao negar a presença de soldados na Crimeia, a Rússia conseguiu retardar a reação ucraniana e ocupar posições estratégicas (SNEGOVAYA, 2015).

Mas, como a Guerra de Informação russa, apoiada em uma forte componente de desinformação, foi conduzida? Quais os principais meios empregados? Qual o conteúdo dessa desinformação e qual seu público alvo? É o que veremos a seguir.

[102] Controle reflexivo envolve técnicas para induzir um adversário a escolher, voluntariamente, ações mais vantajosas para os objetivos russos, moldando as percepções do adversário sobre a situação (SNEGOVAYA, 2015)

5.1.1 A Guerra de Informação Russa

A desinformação, a manipulação e a propaganda foram armas amplamente empregadas pela Rússia contra a Ucrânia, por meio de mensagens bem ajustadas ao público-alvo tanto dentro do seu próprio país, quanto na Ucrânia e no exterior (KOFMAN *et al*, 2017; PAUL *et al*, 2018). A Rússia se valeu da difusão da língua e da cultura russas na Ucrânia para tentar garantir apoio popular para suas ações militares e enfraquecer a resposta do governo (PERRY, 2015). Ao mesmo tempo, procurou controlar a narrativa internacional, negando e, posteriormente, justificando suas ações pela defesa do povo ucraniano de etnia russa ou russófono (PERRY, 2015).[103]

A construção da desinformação russa era baseada na combinação de informações verdadeiras junto com mentiras (SAZONOV *et al*, 2016). Isso permitia que as pessoas reconhecessem um fato familiar e, por associação, elas estariam preparadas a confiar no resto da informação, que era na verdade manipulada (SAZONOV *et al*, 2016). Algumas técnicas foram empregadas para facilitar a assimilação das informações pela população em geral. Uma técnica bastante recorrente foi a construção de histórias de interesse humano, tendo como alvo pessoas de diferentes níveis culturais e com pouco interesse por políticas complexas (LUCAS; POMERANTSEV, 2016).

Os canais empregados para disseminação das informações também eram um fator sensível dessa estratégia. Após sua construção, a informação era divulgada por canais ligados à Rússia, até que fosse publicada por meios independentes, sem conexão com o país, de modo que, pelo menos para alguns leitores, aumentasse o grau de credibilidade dessa informação (LUCAS; POMERANTSEV, 2016). Uma amostragem dos canais empregados pela desinformação russa encontra-se no QUADRO 7 (ANEXO C – Canais mais importantes para a desinformação russa).

Em 2014, o instrumento mais importante da desinformação russa era a televisão, mas a internet também desempenhou um papel significativo (SAZONOV *et al*, 2016). As mídias sociais foram empregadas com grande eficácia para espalhar significativa quantidade de desinformação (KOFMAN *et al*, 2017). Duas das plataformas de mídia social mais populares da Ucrânia tiveram páginas pró-Maidan bloqueadas,[104] pois eram hospedadas em servidores russos, e foram forçadas a compartilhar informações dos usuários que se mostravam favoráveis ao conteúdo delas (KOFMAN *et al*, 2017).

---

[103] Pessoa que fala russo (www.dicionarioweb.com.br).
[104] VKontakte e Odnoklassniki.

Para JONES (2015), o uso generalizado de *bots* e *trolls* talvez tenha sido o aspecto mais inovador do conflito na Ucrânia.[105] [106] Ambos foram empregados para saturar os fóruns de discussão online, influenciá-los com um discurso pró-Rússia e espalhar informações incorretas (JONES, 2015; SEDDON, 2014; POMERANTSEV; WEISS, 2014; CHEN, 2015). O jornal The Guardian chegava a ter quarenta mil comentários por dia em suas reportagens sobre o conflito (POMERANTSEV; WEISS, 2014). Segundo Levinson (2015), era mais importante distorcer as informações e gerar nervosismo entre o público europeu, do que efetivamente vender uma visão específica de mundo.

De acordo com Perry (2015), a Agência de Pesquisa da Internet,[107] com sede em São Petesburgo, com um orçamento de US$ 10 milhões e cerca de mil funcionários em 2015, seria o órgão por trás dessas mensagens. Ele também afirma que suas atividades eram monitoradas e supervisionadas pelo Centro de Segurança de Informação do Serviço de Segurança Federal (FSB, em russo),[108] principal agência de segurança da Rússia.

Além de servir de cortina de fumaça para a presença militar russa na Criméia e no Leste do país,[109] de acordo com Pomeranzev e Lucas (2016), a desinformação foi usada pela Rússia para corroer a imagem do governo ucraniano, enfraquecer o moral e a confiança da população, principalmente das Forças Armadas, reforçar a divisão social entre os grupos favoráveis e contrários à Rússia e degradar o ambiente informacional. Segundo Sazonov *et all* (2016), seu objetivo era criar pânico entre a população, semear a desconfiança entre o governo e as Forças Armadas e desmoralizar as tropas. Já para Kofman *et all* (2017), os objetivos envolviam o descrédito ao novo governo, o grave perigo que este representava para as etnias russas na Ucrânia e a defesa do retorno da Crimeia à influência russa.

Para atingir esses objetivos, a estratégia de desinformação russa adotou narrativas, centradas em ideias-força específicas. Uma dessas narrativas focou na ideia de que houve um golpe de estado na Ucrânia, quando uma junta fascista apoiada pelo ocidente tomou o poder do governo legítimo (LUCAS; POMERANSEV, 2016; POMERANSEV; WEISS, 2014). Essa narrativa visava destruir o apoio interno e internacional ao novo governo, em particular da Europa e da OTAN, mostrando a imagem de um governo ilegítimo em um Estado falido

---

[105] *Bots* são aplicações autônomas que rodam na internet enquanto desempenham algum tipo de tarefa pré-determinada. Eles podem ser úteis e inofensivos para os usuários em geral, mas também podem ser usados de forma abusiva por criminosos (https://www.techtudo.com.br/noticias/2018/07/o-que-e-bot-conheca-os-robos-que-estao-dominando-a-internet.ghtml).

[106] Pessoa cujo comportamento tende a desestabilizar uma discussão e irritar outras pessoas na internet, (https://www.techtudo.com.br/artigos/noticia/2013/06/o-que-sao-trolls-e-o-que-e-trollagem.html).

[107] *Internet Research Agency*, tradução nossa.

[108] *Federal Security Service (FSB) Information Security Center*, tradução nossa.

[109] Em uma entrevista coletiva em 4 de março de 2014, Putin disse que seu país não tinha planos de anexar a Crimeia e que não havia soldados russos em solo da Crimeia (KOFMAN *et al*, 2016l).

(LUCAS; POMERANSEV, 2016; POMERANTSEV, 2015). Visava, também, incentivar seu público interno e enfraquecer resistências internas às suas ações (LUCAS; POMERANSEV, 2016).

Uma segunda narrativa foi construída em torno da ideia da Novorossiya,[110] um conceito antigo reavivado pelo presidente Putin em 2014 (KOFMAN *et al*, 2017; POMERANSEV; WEISS, 2014). O termo, de conotações históricas, serviu para legitimar as ações dos separatistas do Leste da Ucrânia e auxiliou os líderes russos a promoverem a causa na região (KOFMAN *et al*, 2017). Com o decorrer do conflito, essa narrativa foi sendo abandonada, em boa parte devido a sua superficialidade, mas também para ajustar um discurso conciliatório que facilitasse a assinatura dos acordos de Minsk, em setembro de 2014 (KOFMAN *et al*, 2017; JAITNER, 2015).

Por fim, a terceira narrativa era focada nas Forças Armadas da Ucrânia e nos batalhões de voluntários, mais precisamente em degradar sua imagem, empregando diversos métodos e técnicas para afetar o moral dos soldados e oficiais ucranianos (SAZONOV *et al*, 2017). As reportagens e artigos citavam delitos e crimes, como execuções, assassinatos e torturas, que teriam sido cometidos pelas tropas contra a parcela da população que falava russo, mas que nunca foram comprovados (SAZONOV *et al*, 2017). Também faziam referências à ineficiência e incapacidade dos seus militares, dos voluntários e de seus comandantes (SAZONOV *et al*, 2017).

Exemplos dessa desinformação podiam ser encontrados no site do jornal Komsomolskaya Pravda, que se referia abertamente aos militares como “criminosos, estupradores, viciados em drogas, alcoólatras, ladrões e covardes que insultam e torturam mulheres, crianças e idosos” (SAZONOV *et al*, 2016, p. 85, tradução nossa). Imagens de prisioneiros de guerra desmoralizados e reservistas inseguros eram mostradas em certos canais de televisão e operadoras de telefonia móvel, que em sua maioria são controladas por capital russo, enviavam mensagens depreciativas e ameaçadoras para os soldados e seus familiares (SAZONOV *et al*, 2017). Dentro do contexto dessas narrativas, o QUADRO 8 (ANEXO D – Principais temas empregados nas campanhas de desinformação) apresenta outros temas empregados na campanha de desinformação:

A campanha de desinformação russa na Ucrânia empregou uma grande variedade de técnicas e adaptou suas mensagens a diferentes audiências, tornando-as interessantes e

[110] Historicamente uma região ao norte do Mar Negro, anexada pelo Império Russo após as guerras Russo-turcas. O termo foi revivido para denotar uma confederação da autoproclamada República Popular de Donetsk e da República Popular de Lugansk, no leste da Ucrânia (JAITNER, 2015).

emocionalmente envolventes para o público em geral, mesmo se tratando de mentiras descaradas. Para torná-las atraentes, a Rússia estava preparada para fabricar inteiramente suas estórias, empregando fotos e vídeos reais, fora de contexto ou intencionalmente produzidos. Além disso, suas ações se valeram de vários meios de comunicação para promoção de suas narrativas, como mídia impressa, redes sociais e noticiários.

A natureza difusa e dinâmica das campanhas de desinformação torna difícil avaliar, com precisão, seu impacto no conflito. Contudo, é válido considerar que as operações russas desorientaram e dificultaram as ações do incipiente governo ucraniano, frearam o movimento pró-europeu na Ucrânia e impediram que a UE, os EUA e a OTAN forjassem uma coalizão militar para se oporem à anexação da Criméia e abafarem as inquietações no Leste do país.

Por ser o principal exemplo de uma campanha de desinformação inserida no contexto de uma Guerra Híbrida, as ações da Rússia na Ucrânia se tornam uma referência importante na avaliação de futuras estratégias de combate à desinformação. Assim, abordaremos a estratégia proposta neste trabalho à luz dessa situação específica.

5.2 A Análise da Estratégia Proposta

A estratégia proposta no capítulo anterior para combater a desinformação foi formulada com base em estratégias criadas dentro do cenário europeu, posteriormente ao conflito na Ucrânia. Assim, é natural que as ações da Rússia tenham influenciado sua elaboração, embora os documentos estudados não deixem isso explícito. Mesmo assim, o confronto dos objetivos e ações propostos com os eventos ocorridos na Ucrânia em 2014 é importante para validar a estratégia e poderá agregar *insights* importantes à sua implementação. Dessa forma, passaremos a analisar cada um dos objetivos propostos.

5.2.1 Desenvolver a Capacidade de Detectar, Analisar e Expor a Desinformação

O primeiro passo para enfrentar uma ameaça é identificá-la e reconhecê-la como tal. Como citado anteriormente neste capítulo, a desinformação russa era bem produzida e procurava combinar informações falsas com fatos verdadeiros, o que tornava sua detecção mais difícil. Também como já visto anteriormente, esse esforço torna-se ainda mais complicado em um ambiente de Guerra Híbrida, onde o agressor busca disfarçar suas intenções sob o manto da negação plausível e da ambiguidade.

À época do conflito, a Ucrânia não dispunha de um órgão vocacionado para a

detecção e análise da desinformação. Quando os efeitos da campanha de desinformação passaram a ser sentidos, algumas ONG e instituições civis foram criadas pela própria sociedade para, justamente, tentar se contrapor a essa ameaça (KURK, 2017).[111] Porém, essas iniciativas tinham sua eficácia reduzida pela dificuldade de coordenar as ações das entidades civis e do governo e pela dificuldade de obter informações precisas em uma região em conflito (KURK, 2017).

Essas limitações poderiam ser minimizadas pela existência de um órgão governamental, vinculado à área de inteligência, que pudesse monitorar tanto o ambiente interno quanto o internacional, canalizando as informações das diversas fontes. Com uma composição multidisciplinar, esse órgão teria a capacidade de analisar as informações difundidas, identificar suas inconsistências e buscar os fatos reais por trás das desinformações. Tal órgão também serviria como um ponto de ligação para o apoio dos EUA, da UE e da OTAN ao esforço de combate à desinformação.

A capacidade de inteligência do governo também seria importante para analisar as fontes que originaram as desinformações. Todos os canais citados no QUADRO 7 (ANEXO C — Canais mais importantes para a desinformação russa) poderiam ser monitorados e investigados, inclusive quanto ao seu financiamento. O emprego de *trolls* e *bots* poderia ser comprovado e exposto ao público em geral. Indícios de ligações entre essas fontes e outras fontes anônimas de desinformação com a Rússia ou com os grupos separatistas no Leste do país teriam ajudado a desacreditá-las e a chamar a atenção da população e da comunidade internacional para o problema.

Dessa forma, é possível afirmarmos que, com uma agência governamental coordenando as ações dos setores do governo e da sociedade, as ações de detecção e análise da campanha de desinformação russa teriam sido muito mais eficazes, rápidas e confiáveis, permitindo melhorar sua capacidade de resposta e reduzir os efeitos negativos da desinformação. Por outro lado, no contexto específico da Ucrânia, cujas dimensões e organização estão distantes daquelas encontradas na UE ou em um país como o Brasil, não se visualiza nenhum ganho específico no estabelecimento de um Sistema de Alerta Rápido.

5.2.2 Empregar a Comunicação Estratégica de Maneira Eficaz

A guerra da desinformação é uma guerra de narrativas, onde o momento e o canal

[111] Como a StopFake, o Ukraine Crisis Media Center, a Informnapalm, a Euromaidan Press e a Informacijnyi Sprotyv (KURK, 2017).

são tão importantes quanto o conteúdo. Para isso, o emprego eficaz de comunicações estratégicas é uma parte integral da resposta à desinformação, tanto para a construção da resiliência da sociedade quanto para combater narrativas falsas, como as que foram exploradas pela Rússia (COMISSÃO EUROPEIA, 2018b). Essas comunicações devem ser baseadas em fatos e sua disseminação precisa ser oportuna, não dando tempo para que a desinformação seja interpretada pela audiência nacional e internacional como uma verdade.

Antes do conflito de 2014, não foi identificada uma preocupação específica da Ucrânia em desenvolver suas comunicações estratégicas. Quando as ações da Rússia começaram, uma completa mudança de poder estava ocorrendo na Ucrânia. Por isso, enquanto o novo governo estava sendo formado, a capacidade de reação ucraniana à desinformação russa estava muito limitada (KURK, 2017). Por outro lado, a Rússia, desde a época da União Soviética, já fazia uso da propaganda e da desinformação. Assim, o governo russo conseguiu assumir o controle da narrativa e mantê-lo até o final do conflito.

Dessa forma, se a Ucrânia tivesse um órgão especializado no emprego das comunicações estratégicas talvez pudesse ter impedido o sucesso da desinformação russa. Em primeiro lugar, esse órgão poderia ser empregado como um ponto focal do governo para conduzir campanhas de educação e orientação da população contra a desinformação. Poderia, também, produzir campanhas de propaganda das ações do governo, focando nos benefícios para a população dessas ações e mostrando que a Ucrânia estava longe de ser um Estado falido, apesar da crise política e social. Poderia, ainda, ser empregado para atenuar as tensões sociais, principalmente no que tange à população de origem russa ou russófona.

Além disso, por ser um órgão técnico, ele teria condições de, em conjunto com a detecção e análise da desinformação, auxiliar o governo em formação no combate às campanhas de desinformação. Esse auxílio envolveria o desenvolvimento de estratégias para se contrapor a cada uma das narrativas russas, definindo os melhores conteúdos e canais para esse fim.

Por melhor que seja a mensagem, ela não surtirá efeito de não tiver credibilidade e se não alcançar o público em geral. Para que isso aconteça, uma ampla rede de comunicadores, que contem com a confiança da população, é fundamental para dar maior credibilidade às informações que estão sendo passadas pelo governo e amplitude à sua disseminação. Nesse sentido, o governo ucraniano contou com certo apoio das ONG e instituições civis citadas anteriormente. Porém, novamente, a ausência de um órgão vocacionado para à comunicação limitou a eficácia dessas medidas.

Um bom exemplo da importância das comunicações estratégicas para enfrentar a desinformação foi a campanha de difamação e desmoralização das Forças Armadas. A

desinformação russa se aproveitou dos baixos índices de aprovação que as Forças Armadas da Ucrânia possuíam (KURK, 2017) para explorar essa vulnerabilidade e atuar no domínio cognitivo dos militares. Tal fato poderia ter sido evitado ou atenuado se, antes do conflito, houvesse a preocupação de melhorar a percepção da população sobre suas Forças Armadas por meio de uma campanha de comunicação estratégica.

Essa situação começou a mudar com a mobilização de voluntários no conflito, quando passou a haver uma maior identificação da população com as tropas envolvidas no conflito (KURK, 2017). Assim, é possível deduzir que os efeitos dessa campanha sobre a população e os próprios militares poderiam ter sido bastante atenuados se houvesse um trabalho de propaganda para fortalecer a credibilidade dos militares, com base no seu profissionalismo e comprometimento, e para nutrir a confiança dos cidadãos nas instituições.

Prova da importância do emprego de comunicações estratégicas eficazes no combate à desinformação foi o efeito positivo que a ONG *Ukraine Crisis Media Center* (UCMC),[112] em particular, teve no apoio ao governo ucraniano. No caso das Forças Armadas, o UCMC procurou melhorar a percepção sobre suas lideranças, incentivando o serviço nas Forças Armadas e colocando os comandantes militares que estavam em combate para passar informações sobre as atividades desenvolvidas e a situação no Leste (KURK, 2017). Também desenvolveu o projeto *One Voice Policy*,[113] cedendo profissionais de comunicação a diversos setores do governo para fortalecer sua capacidade de comunicação e unificar o discurso.

Assim, para o combate à desinformação, é vital que o Estado amplie a compreensão da população sobre o problema, ao mesmo tempo que eleve sua confiança e apoio às instituições do Estado, em particular aos órgãos de segurança pública e às Forças Armadas. Para isso, o emprego eficaz das comunicações estratégicas é uma condição *sine que non*. O estabelecimento de um órgão técnico, com profissionais qualificados, proporcionará as capacidades necessárias para que o governo possa enfrentar a guerra de narrativas de uma campanha de desinformação. Esse órgão técnico poderia combinar os esforços de detecção e análise com a comunicação estratégica, desde que devidamente estruturado e mobiliado por pessoal qualificado para ambas as tarefas.

5.2.3 Mobilizar o Setor Privado

Na guerra de narrativas, ações ativas do governo no campo das comunicações

[112] Centro de Mídia da Crise da Ucrânia, tradução nossa.
[113] Política da Voz Única, tradução nossa (RINGIS, 2014, apud KURK, 2017).

estratégicas representam apenas um dos eixos do esforço a ser desenvolvido. Um segundo eixo deve envolver ações para impedir que o oponente faça uso do ambiente midiático para disseminar sua desinformação e propaganda.

No conflito com a Ucrânia, a Rússia valeu-se da penetração da programação de suas redes de rádio e televisão no país e no exterior para espalhar sua desinformação. Quando identificou essa vulnerabilidade, o governo ucraniano baniu a concessão dessas empresas, limitando sua influência nesse ambiente, reduzindo o alcance e amplitude das ações russas (KURK, 2017).

Contudo, o mesmo não pôde ser feito com a internet. Os sites e redes sociais hospedados em servidores russos ou sustentados por capital russo continuaram operando normalmente. Além disso, a desinformação russa circulava sem restrições pelos demais sites e plataformas, com o emprego de *bots* e *trolls* a lhe dar visibilidade e relevância nos sites de busca e nos fóruns de discussão.

A desinformação se aproveita de um ambiente digital caracterizado pela falta de transparência e de rastreabilidade. Quanto mais difícil verificar a veracidade de uma informação e a confiabilidade de sua fonte, mais fácil é criar, amplificar e disseminar a desinformação. Assim, se não houver ações direcionadas a modificar essas condições, o combate à desinformação será bastante degradado.

A simples elaboração de normas e regulamentos não garante o efeito desejado, uma vez que estes tenderiam a ser ineficientes, incapazes de abarcar todo o espectro de conteúdo empregado na desinformação. Haveria, assim, uma grande dependência das ações das próprias empresas e plataformas. Como visto no capítulo anterior, é necessário conscientizar e mobilizar o setor privado para promover as mudanças necessárias, como a UE conseguiu fazer com seu Código de Práticas.

Se, à época do conflito, houvesse um compromisso similar por parte dos administradores dos sites de notícias e das plataformas sociais para proteger os usuários da desinformação, é possível afirmarmos que o governo ucraniano, as ONG e instituições civis envolvidas no combate à essa ameaça estariam melhor equipadas para lidar com a situação.

Em primeiro lugar, os usuários teriam melhores condições de chegar a conclusões esclarecidas sobre um tópico, baseadas no pensamento crítico, tendo acesso a informações diversificadas e com abordagens diversas e alternativas sobre os assuntos, e não um discurso único. Além disso, essas conclusões levariam em consideração as intenções por trás de uma determinada informação, facilitadas pela identificação da origem da informação, principalmente quando envolver conteúdo ou site patrocinado.

Outras ferramentas que poderiam estar à disposição dos usuários seriam indicadores da confiabilidade e da natureza de uma fonte. A indicação da confiabilidade da origem da informação poderia ser feita com base no seu histórico de postagens, da mesma forma que é feito em alguns sites de compra, onde uma avaliação do vendedor está disponível ao comprador, com base em alguns parâmetros, como quantidade de vendas, atendimento e respeito ao prazo de entrega. De maneira análoga, a origem da informação teria sua confiabilidade indicada, considerando, por exemplo, a quantidade de mensagens já postadas e o percentual de informações falsas já identificadas. A outra ferramenta procuraria identificar quando a informação fosse originada em *bots*, de modo que os usuários possam desconsiderar o conteúdo postado. Ferramentas online para verificar se fotos e vídeos são falsos ou não também poderiam ser disponibilizadas aos usuários.

Uma segunda vantagem da mobilização do setor privado no combate à desinformação envolveria a atividade de verificação de fatos. As organizações governamentais e civis envolvidas dessa atividade poderiam ter acesso aos dados das plataformas, respeitando a privacidade dos usuários e a propriedade intelectual, de modo a poderem identificar e mapear os mecanismos empregados na desinformação e avaliar o impacto causado por elas, melhorando a eficiência do processo.

Por último, o comprometimento das plataformas online teria reduzido a efetividade dos trolls russos por meio do cancelamento de contas e perfis falsos utilizados por eles para amplificarem o efeito de suas postagens. Além disso, teria contribuído para desestimular que os sites e usuários retransmitissem informações das quais não tivessem certeza quanto a sua veracidade, adotando medidas para reforçar a prestação de contas e pela exposição dos sites e das contas envolvidas na disseminação da desinformação. Por outro lado, as plataformas online poderiam adotar medidas para evitar que a Rússia tivesse acesso aos dados dos usuários ucranianos, como aconteceu com as plataformas sociais VKontakte e Odnoklassniki.

Assim, levando em consideração as medidas aqui apresentadas, que poderiam ter sido adotadas pelas plataformas digitais, a exemplo do que vem sendo adotado na UE, podemos supor que elas poderiam ter efeitos positivos nos esforços ucranianos para enfrentar a desinformação.

5.2.4 Fortalecer o Ambiente Midiático

O ambiente informacional midiático é caracterizado pelo conjunto dos indivíduos, organizações e sistemas, vinculados aos meios de comunicação, que coletam, processam e

disseminam a informação. A livre circulação de ideias, a difusão de informações de qualidade e a existência de meios de comunicação confiáveis são condições que contribuem para reforçar a resiliência desse ambiente, dificultando a disseminação da desinformação e favorecendo o seu combate.

Nesse sentido, o primeiro passo é assegurar que esse ambiente midiático seja estruturado com base na liberdade de expressão e de imprensa e que propicie o pluralismo de ideias e de informações. Tanto o governo quanto a sociedade são responsáveis por garantir que isso aconteça. O primeiro deve assegurar a proteção de fato e de direito desses princípios, não interferindo na independência editorial das organizações, nem limitando o acesso a nenhuma fonte legítima. Já à sociedade cabe cobrar do governo essas garantias.

No contexto da Ucrânia, não é possível afirmarmos que houvesse qualquer tipo de interferência nessas liberdades por parte do governo. Contudo, a grande participação das mídias russas nesse cenário, seguindo as orientações do governo russo, via FSB, limitava a diversidade do debate e das informações. Além disso, o controle russo sobre parcela das redes sociais da Ucrânia definitivamente restringiu a liberdade de expressão de seus opositores.

O segundo passo para fortalecer o ambiente midiático é incentivar a produção e disseminação de informações de qualidade em plataformas confiáveis. Para isso, profissionais bem qualificados são fundamentais, com conhecimento não só sobre os fundamentos do jornalismo e da comunicação, mas também sobre as habilidades digitais necessárias ao ambiente atual, sobre os valores éticos e morais da profissão e, particularmente, sobre a desinformação. Da mesma forma, as plataformas devem ser incentivadas a verificar e a se responsabilizar pelo conteúdo publicado. Aqueles que não respeitarem esses preceitos devem ser desacreditados perante a população e levados a prestar conta de seus atos, inclusive por meio da adoção de medidas legais.

Não foi possível obter dados sobre a formação e a qualificação dos profissionais da mídia na Ucrânia nessa época. Contudo, a percepção que se tem pelo desenrolar das ações é que eles não estavam preparados para lidar com o volume e intensidade da campanha de desinformação russa. Ainda assim, as primeiras respostas à essa campanha vieram de especialistas da área de comunicações estratégicas, relações públicas e relações internacionais, que criaram organizações como o *Ukraine Crisis Media Centre* e o site *StopFake* (KURK, 2017), o que confirma a existência de profissionais preparados na Ucrânia, mesmo que não seja possível afirmar que essa fosse a regra. Ainda assim, sempre há margem para aperfeiçoamento.

Prova disso foram as ações adotadas pelo Ministério da Política da Informação,[114] que introduziu novas qualificações nas universidades nas áreas de ciência da comunicação e de comunicações de mídia (KURK, 2017).

Porém, mais uma vez, os meios de comunicação, as plataformas online, os profissionais, os influenciadores e os usuários em geral ligados à Rússia, além dos *bots* e *trolls*, exploraram a falta de proteção do ambiente midiático ucraniano e conseguiram, durante a maior parte do período do conflito, disseminar informações falsas, confundindo a população e enfraquecendo sua confiança na mídia.

Um ambiente midiático saudável também é decorrente da participação da sociedade, que deve exigir de quem produz e distribui as informações uma conduta ética, profissional e precisa, justificando a confiança neles depositadas. Para que isso ocorra, a sociedade deve desenvolver mecanismos que permitam a verificação da veracidade dos fatos que estão sendo disseminados, algo que a sociedade ucraniana não possuía no início de 2014.

Quando as agressões russas começaram, o novo governo ucraniano ainda estava se organizando e enfrentou grandes dificuldades para confrontar a desinformação dos russos. Diante da ameaça, diversas iniciativas começaram a surgir na sociedade para apurar a verdade dos fatos, expor as notícias falsas e a propaganda russa, providenciar informações confiáveis sobre os acontecimentos e bloquear as mensagens de *trolls* (KURK, 2017). Foram criadas ferramentas online para permitir aos usuários identificarem fotos e vídeos falsos e combaterem conteúdos falsos (KURK, 2017).

Mais uma vez, é difícil dimensionar o efeito dessas iniciativas na campanha conduzida pela Rússia. As respostas da sociedade ucraniana, ilustradas anteriormente, podem não ter sido suficientes para resolver o problema, mas com certeza contribuíram para fortalecer sua capacidade para lidar com a desinformação e reduzir sua eficácia.

Os aspectos apresentados neste item reforçam a importância de ações direcionadas à construção de um ambiente midiático forte, seguro e confiável. Apesar de não poder ser considerado desestruturado, o ambiente midiático ucraniano encontrava-se vulnerável à desinformação russa devido à forte influência dos meios de comunicação russos no país. Ainda assim, se as organizações e profissionais de mídia estivessem melhor preparadas e a sociedade ucraniana mais consciente da ameaça que essa presença representava, é plausível considerar que seus efeitos fossem bastante atenuados ou, até mesmo evitados.

[114] Do original *Ministre of Information Policy*, tradução nossa. (KURK, 2017).

5.2.5 Desenvolver a Resiliência

A última componente da estratégia proposta está relacionada ao desenvolvimento da resiliência da sociedade. Para KURK (2017), em sociedades com elevado grau de conscientização e resiliência, os efeitos da desinformação são atenuados. Para prosperar, a desinformação precisa encontrar solo fértil em um ambiente vulnerável, tanto no ambiente midiático, quanto no domínio cognitivo da sociedade. O primeiro foi abordado no item anterior. Vamos, agora, tratar de ações que podem ser adotadas para atenuar a vulnerabilidade da sociedade a essa ameaça.

Para combater a desinformação, particularmente diante da vasta gama de informações disponíveis nas mídias, as pessoas devem ser capazes de diferenciar fatos de opiniões, compartilhando essas informações de forma responsável. Para isso, não basta apenas sermos capazes de acessar as informações. É necessário identificar a autoria, analisar o contexto e interpretar sua intenção.

A educação midiática envolve o desenvolvimento de "habilidades para acessar, analisar, criar e participar de maneira crítica do ambiente informacional e midiático em todos os seus formatos – dos impressos aos digitais" (Site EDUCAMIDIA).[115] Ela ajuda a população a desenvolver o pensamento crítico sobre o conteúdo difundido pela mídia e, com isso, enfraquecendo o alcance e os efeitos de notícias falsas e a manipulação da verdade. Se inserirmos nesse processo uma melhor compreensão e conscientização sobre o problema da desinformação, teremos, com certeza, uma audiência melhor preparada para interpretar as informações dentro do contexto adequado.

Diante dos reflexos do desenvolvimento tecnológico no ambiente midiático, torna-se importante, também, desenvolver a educação digital da população. Por exemplo, compreender o que são *bots* e *trolls* e como eles podem afetar a percepção da sociedade sobre um determinado assunto ou como imagens e vídeos podem ser alterados são capacidades importantes para o juízo de valor que devemos fazer sobre as informações que nos são transmitidas.

Se ações nesse sentido tivessem sido adotas pelo governo da Ucrânia, é coerente avaliarmos que as narrativas russas para deslegitimar o governo ucraniano, para caracterizar a Ucrânia como um Estado falido, para negar a participação de tropas russa no conflito poderiam ser contestadas por maior parcela da população. Acusações sobre atos criminosos ou

[115] www.educamidia.org.br.

inapropriados das forças ucranianas não seriam aceitas pela sociedade sem a devida comprovação dos fatos, evitando o desgaste desnecessário do governo e a falta de confiança nos militares. Além disso, as fontes da desinformação poderiam ser melhor expostas e desacreditadas.

Um segundo fator importante da resiliência da sociedade contra a desinformação é a construção de um arcabouço legal atualizado. Além de contar com a colaboração do setor privado, o governo deve dispor dos meios para enfrentar a desinformação e a propaganda que promove o ódio e a intolerância. Para isso, o amparo de uma legislação bem ajustada será fundamental.

Leis que tenham sido elaboradas antes das inovações do ambiente midiático e fora do contexto da ameaça imposta pela desinformação podem deixar de abordar aspectos importantes relacionados à proteção de dados pessoais e empresariais, à concessão e cancelamento de licenças para o funcionamento dos meios de comunicação, principalmente vinculados à capital estrangeiro ou hospedados no exterior, à difusão de conteúdo ilícito, assim como a própria definição de conteúdo ilícito, entre outros. Assim, uma ampla revisão desse arcabouço poderia ajudar a identificar vulnerabilidades que possam ser exploradas por um agressor híbrido. Para esse fim, o apoio de especialistas nas áreas de comunicações, mídia e propaganda seria primordial.

Como já analisamos, a forte presença russa no ambiente midiático da Ucrânia foi um dos fatores que contribuiu para facilitar suas ações de desinformação. O controle de plataformas digitais e o emprego de *bots* e *trolls* foi outro fator. Se a legislação ucraniana estivesse ajustada a uma possível ameaça híbrida, essa presença russa poderia ter sido restringida ou mecanismos para o banimento dos seus meios de comunicação poderiam agilizar uma resposta. Além disso, a previsão de responsabilização e punição para os indivíduos e instituições envolvidos na criação e difusão da desinformação poderia desestimular a participação nesse processo, principalmente no ambiente virtual.

Uma avaliação mais completa da eficácia dessa medida dependeria de uma análise mais detalhada do arcabouço jurídico ucraniano, o que fugiria do escopo deste trabalho. Mesmo assim, os exemplos apresentados acima nos permitem perceber que uma revisão da legislação do país poderia ter melhorado a resiliência contra campanhas de desinformação, dificultando as ações da Rússia e facilitando a resposta ucraniana.

O terceiro fator a ser fortalecido para contribuir para a resiliência da sociedade são as divisões sociais do país, que podem ser exploradas na Guerra Híbrida, principalmente por meio de campanhas de desinformação e propaganda. As sociedades devem identificar essas

insatisfações internas e atuar de maneira incisiva sobre suas causas, de modo a não permitir sua exploração.

Um exemplo claro desse aspecto foram as ações da Rússia sobre a população russófona na Ucrânia. A polarização do país entre o ocidente e a Rússia era repetida na população, onde a minoria da etnia russa, concentrada no Leste e no Sul do país se sentia ameaçada com a aproximação com o Ocidente. Assim, a desinformação russa se aproveitou desse temor e tentou buscar apoio a suas ações junto a essa parcela da população, disseminando informações de que ela estaria sob ameaça de um governo ultranacionalista violento e de que as Forças Armadas estariam cometendo atrocidades contra eles.

É obvio que o governo recém empossado da Ucrânia em 2014 não tinha tido tempo para lidar com a questão, mas se governos anteriores houvessem tentado combater essa polarização e proporcionado maior inclusão à população russófona, é bem possível que a desinformação russa não encontra-se as fraturas no tecido social à época do conflito. Portanto, é válido afirmar que avaliar as tensões, polarizações e insatisfações dentro da sociedade e procurar lidar com essas questões contribuirá para a resiliência e auxiliará no combate à desinformação.

O último fator tratado está relacionado à resiliência das Forças Armadas. Como já abordado neste capítulo, uma das narrativas principais da desinformação russa era voltada para degradar a confiança da população nos militares e dos próprios militares nas suas capacidades e nas suas lideranças. Ela se aproveitou de uma imagem já negativa que a sociedade ucraniana tinha das Forças Armadas e procurou reforçar essa percepção.

Os efeitos da narrativa teriam sido bastante atenuados se a imagem das Forças Armadas fosse melhor trabalhada, como proposto quando falamos sobre as comunicações estratégicas. Além disso, um trabalho de fortalecimento interno dos militares deve ser uma preocupação constante de sua liderança, com ações direcionadas para desenvolver a liderança, elevar o moral, reforçar a disciplina e valorizando o profissionalismo. Para avaliar os resultados dessas medidas e identificar aspectos a serem melhorados, deve ser feito o acompanhamento constante do ambiente interno e o monitoramento de influências externas negativas.

O propósito de todas as ações direcionadas ao desenvolvimento da resiliência é blindar a sociedade contra os esforços de um agressor para explorar suas vulnerabilidades por meio da desinformação. Para isso, promover a educação midiática e digital e aumentar a conscientização sobre a desinformação permitirão que as pessoas avaliam as informações com senso crítico. A revisão do arcabouço legal proporcionará melhores condições para proteger o ambiente e responder a eventuais ataques. O combate às divisões sociais evitará que a

desinformação se aproveite de tensões e polarizações internas. E, por último, o fortalecimento da imagem das Forças Armadas irá evitar a degradação de sua capacidade de combate pela desinformação.

5.3 Conclusões Parciais

As ações de Guerra Híbrida da Rússia na Ucrânia foram consideradas o paradigma desse tipo de conflito. Nesse contexto, sua campanha de desinformação também foi considerada, por muitos autores, como um exemplo da condução dessa atividade. Empregando uma grande variedade de canais e disseminando informações bem ajustadas às diversas audiências, a Rússia estabeleceu narrativas que buscavam confundir quanto ao seu envolvimento direto no conflito, principalmente no Leste do país, conquistar o apoio do povo russo e dos russófonos da Ucrânia, particularmente para a anexação da Criméia, desacreditar e enfraquecer o governo ucraniano e fragilizar o moral e a credibilidade das Forças Armadas da Ucrânia.

Um aspecto de destaque da campanha de desinformação russa foi o emprego das plataformas digitais, tanto o site dos meios de comunicações quanto as mídias sociais. Nesse setor, a atuação de *bots* e *trolls* foi um fator que contribuiu sobremaneira para sobrecarregar o ambiente informacional com informações falsas sobre os fatos que estavam ocorrendo, contribuindo com as narrativas desenvolvidas.

A natureza das ações de desinformação torna difícil avaliar a sua eficácia. Contudo, podemos considerar que as operações russas contribuíram para desorientar e dificultar as ações do incipiente governo ucraniano, frear o movimento pró-europeu na Ucrânia e impedir que a UE, os EUA e a OTAN forjassem uma coalizão militar para se oporem à anexação da Criméia e abafarem as inquietações no Leste do país.

A análise da estratégia proposta no capítulo anterior para o combate à desinformação, à luz da campanha russa, nos permitiu avaliar que os objetivos e ações propostos estão aderentes com as principais vulnerabilidades exploradas pela Rússia. Assim como no caso das ações russas, é difícil avaliar os efeitos da estratégia proposta sobre uma campanha de desinformação. Porém, a análise subjetiva da situação ucraniana nos oferece fortes indícios de que essa estratégia poderia minimizar as vulnerabilidades identificadas. Dessa maneira, é coerente considerarmos que sua adoção poderia ter atenuado os efeitos da desinformação russa e facilitado a execução de eventuais respostas.

Assim, com base nos aspectos apresentados neste capítulo, concluímos que a

estratégia de combate à desinformação proposta neste trabalho traz objetivos e ações capazes de minimizar as vulnerabilidades normalmente exploradas por uma campanha de desinformação e de se contrapor a suas ações.

6 CONCLUSÃO

Nas últimas décadas, diversos conceitos foram desenvolvidos para tentar entender e explicar as mudanças ocorridas na condução dos conflitos armados contemporâneos. O conflito entre a Rússia e a Ucrânia, em 2014, colocou em evidência o conceito da Guerra Híbrida. Desde a formulação das definições iniciais até os dias de hoje, o conceito de Guerra Híbrida sofreu diversas interpretações e evoluiu, acompanhando as mudanças observadas a cada novo conflito.

Atualmente, diversas instituições, principalmente na Europa, têm se dedicado ao estudo desse conceito e desenvolvido estratégias para combatê-lo. Diante de toda a repercussão que o conceito de Guerra Híbrida tem gerado e da possibilidade de sua aplicação dentro do nosso entorno estratégico, visualizamos a necessidade de aprofundar os conhecimentos sobre o assunto, de modo a embasar a adoção de medidas no campo político e estratégico.

Dessa forma, o presente trabalho teve como propósito a investigação de que a ambiguidade gerada pela campanha de desinformação da Rússia contra a Ucrânia em 2014 contribuiu para retardar e enfraquecer a resposta a suas ações e a identificação de ações que possam fazer parte de uma estratégia de combate à desinformação dentro do contexto da Guerra Híbrida. Para isso, buscamos construir um sólido arcabouço teórico sobre o conceito, com ênfase no uso da desinformação. Além disso, identificamos estratégias de combate à Guerra Híbrida e à desinformação, que serviram como referência para a formulação da estratégia proposta. Por fim, analisamos essa estratégia à luz das ações da Rússia contra a Ucrânia.

Assim, para o desenvolvimento do trabalho, no capítulo dois, apresentamos as definições iniciais da Guerra Híbrida e suas principais características. Foram, ainda, abordados os reflexos que as ações da Rússia contra a Ucrânia tiveram sobre o conceito, ampliando o espectro das ações envolvidas.

No entendimento deste autor, de todas as definições apresentadas sobre o conceito, a definição de Reichborn-Kjennerrud e Cullen (2017) foi a que melhor capturou essa ampliação, por considerar o emprego sincronizado de múltiplos instrumentos do poder adaptados a vulnerabilidades específicas em todo o espectro de funções da sociedade para atingir efeitos sinérgicos. Um modelo gráfico foi apresentado para ilustrar a dinâmica da Guerra Híbrida, representando a escalada horizontal e vertical das ações. Encerrando o capítulo, identificamos os principais instrumentos empregados pela Guerra Híbrida. Verificamos que a Guerra de Informação tem se mostrado uma poderosa ferramenta para o domínio do espaço cognitivo e psicológico e que a desinformação, potencializada pelo desenvolvimento tecnológico, pode ser

bastante eficaz para moldar a narrativa do conflito.

No capítulo seguinte, descrevemos o modelo desenvolvido pelo MCDC(CHW) *Project* para a formulação de estratégias de combate à Guerra Híbrida. Esse modelo está estruturado em três componentes: detectar um ataque híbrido; dissuadir ataques híbridos; e responder a ataques híbridos. Para facilitar a compreensão desse modelo e associá-lo a medidas concretas a serem implementadas, traçamos um paralelo, ao longo do capítulo, com a estratégia adotada, em 2016, pela UE. Verificamos que os processos de detecção precisam ser ajustados às particularidades da Guerra Híbrida, que a realização de avaliações de risco e a construção da resiliência são fundamentais para enfrentar ameaças híbridas e que todas as expressões do poder devem ser empregadas na resposta a ataques híbridos

No capítulo quatro, descrevemos as ações desenvolvidas na estratégia de combate à desinformação adotada pela UE e na estratégia proposta pelo *European Values Center for Security Policy* para combater a desinformação. Verificamos que o grande volume de informações e fontes existentes demandam uma estrutura adequada para detecção e análise. Verificamos, também, que o setor privado e a sociedade como um todo têm um papel importante nessas estratégias e que o governo deve ser capaz de se comunicar eficazmente com esses setores e com outros países. Com base na análise dessas inciativas, identificamos os objetivos e ações que estruturaram uma proposta de estratégia que possa ser adotada pelo Brasil. Os objetivos estabelecidos envolvem: desenvolver a capacidade de detectar, analisar e expor a desinformação; empregar a comunicação estratégica de maneira eficaz; mobilizar o setor privado; fortalecer o ambiente midiático; e desenvolver a resiliência.

Por fim, no capítulo cinco, a estratégia proposta foi analisada tendo como referência a campanha de desinformação conduzida pela Rússia contra a Ucrânia em 2014. Para isso, descrevemos as principais ações russas nessa campanha. Em seguida, os objetivos e ações propostos foram analisados, de modo a avaliar se eles conseguiriam neutralizar as vulnerabilidades ucranianas exploradas ou se poderiam amenizar os efeitos da desinformação russa.

Concluímos que a Rússia soube se aproveitar das vantagens assimétricas existentes e de um contexto bastante particular na Ucrânia, onde a grande penetração do ambiente midiático e a existência de uma significativa presença de russófonos na população permitiram-lhe explorar as vulnerabilidades das divisões sociais e políticas daquele momento por meio de sua campanha de desinformação. A natureza das ações de desinformação torna difícil avaliar a sua eficácia. Contudo, podemos considerar que as operações russas lhe deram o controle da narrativa e lhe asseguraram a ambiguidade desejada na Guerra Híbrida.

A análise subjetiva da estratégia proposta para o combate à desinformação realizada no último capítulo, nos permitiu avaliar que os objetivos e ações propostos estão aderentes com as principais vulnerabilidades exploradas pela Rússia. Dessa forma, acreditamos que, se adotada pela Ucrânia, essa estratégia poderia ter atenuado os efeitos da desinformação russa e facilitado a execução de eventuais respostas.

Ao chegar ao fim deste trabalho, concluímos que o conceito da Guerra Híbrida representa bem as evoluções observadas nos conflitos modernos, principalmente no que se refere ao emprego das diversas expressões do poder nacional nos domínios material e cognitivo. Para isso, o uso da desinformação mostra-se uma ferramenta importante na batalha pelo domínio cognitivo. Para evitar que isso aconteça, nos parece oportuno que os Estados estejam preparados para lidar com essa ameaça. Para isso, uma sólida e adaptável estratégia de combate à desinformação é primordial.

Assim, sustentaremos nesta pesquisa a tese de que a desinformação se mostrou uma ferramenta da Guerra Híbrida para gerar ambiguidade quanto à presença e às ações da Rússia contra a Ucrânia, o que contribuiu para retardar e enfraquecer a resposta a suas ações. Além disso, a análise realizada neste trabalho indica que os objetivos e ações aqui propostos para combater a desinformação podem servir como uma base para o desenvolvimento de uma estratégia nacional.

Em particular, a pesquisa sugere que a Marinha do Brasil preste atenção ao continuado fortalecimento da resiliência da instituição e de seu pessoal, para não permitir que as condições exploradas pela desinformação russa contra as Forças Armadas ucranianas se desenvolvam aqui. O fortalecimento da liderança, do moral e da disciplina, preocupações já existentes, possuem o potencial, de acordo com o pesquisado, de reduzir significativamente a eficácia das campanhas de desinformação. Da mesma forma, parece de interesse que seja feito o acompanhamento constante do ambiente interno, de modo a identificar insatisfações e divisões que possam ser exploradas, bem como influências externas que queiram contaminar esse ambiente. Por fim, especial atenção deva ser dada ao desenvolvimento e uso das comunicações estratégicas, mantendo um canal presente e confiável dentro da Força.

Por último, é importante considerar que uma campanha de desinformação pode estar inserida dentro de um contexto mais amplo de emprego de uma estratégia híbrida. É fundamental, então, que medidas de combate à desinformação estejam inseridas, também, dentro de uma estratégia mais ampla de combate à Guerra Híbrida. Assim, sugerimos que a análise de estratégias de combate à Guerra Híbrida para o desenvolvimento de uma estratégia nacional seja objeto de novos estudos.

REFERÊNCIAS

ABBOTT, Katie. *Understanding and Countering Hybrid Warfare: Next Steps for the North Atlantic Treaty Organization*. Ottawa: University of Ottawa, Mar.2016. Disponível em: <https://ruor.uottawa.ca/bitstream/10393/34813/1/ABBOTT%2C%20Kathleen%2020161.pdf>. Acesso em: 10JUN2020.

ARONSSON, Albin. *The state of current counter-hybrid warfare policy*. Londres: MCDC Countering Hybrid Warfare Project, Mar.2019. Disponível em: < https://assets. publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795220/20190304-MCDC_CHW_Info_note_6.pdf>. Acesso em: 12FEV2020.

CHIVVIS, Christopher S. *Understanding Russian 'Hybrid Warfare' And What Can Be Done About it.*Santa Monica, CA, RAND Corporation, Mar.2017. Disponível em: <https://www.rand.org/pubs/testimonies/CT468.html>. Acesso em:07JUN2020.

COMISSÃO EUROPEIA. *Action Plan against Disinformation*. Bruxelas, 2018a. Disponível em: <https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf>. Acesso em: 27JUN2020.

COMISSÃO EUROPEIA. *EU Code of Practice on Disinformation*. Bruxelas, 2018b. Disponível em: <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>. Acesso em: 27JUN2020.

COMISSÃO EUROPEIA. *Communication on tackling online disinformation: a European Approach*. Bruxelas, 2018c. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236>. Acesso em: 22AGO2020.

COMISSÃO EUROPEIA. *Joint Framework on Countering Hybrid Threats - A European Union Response*. Bruxelas, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EM>. Acesso em: 15FEV2020.

COMISSÃO EUROPEIA. *Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats – a European Union response*. Bruxelas, 2017. Disponível em: <https://op.europa.eu/en/publication-detail/-/publication/252e64fb-6d2e-11e7-b2f2-01aa75ed71a1/language-en>. Acesso em: 27JUN2020.

COMISSÃO EUROPEIA. *Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018*. Bruxelas, 2018d. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0014&from=EM>. Acesso em: 02JUL2020.

COMISSÃO EUROPEIA. *Joint Staff Working Document. Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats*. Bruxelas, Bélgica, 2019. Disponível em: < https://www.statewatch.org/media/documents/news/2019/jun/eu-com-hr-implementation-report-hybrid-threats-swd-2019-200.pdf>. Acesso em: 15FEV2020.

COMISSÃO EUROPEIA. *Report on Progress - Action Plan on Disinformation*. Bruxelas, 2019b. Disponível em: <https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf>. Acesso em: 15FEV2020.

EUROPEAN VALUES THINK TANK. *Full-Scale Democratic Response to Hostile Disinformation Operations: 50 Measures to Oust Kremlin Hostile Disinformation Influence out of Europe*. Praga, República Tcheca, 2016. Disponível em: <https://www.kremlinwatch.eu/our-reports/>. Acesso em:16FEV2020.

FIOTT, Daniel; PARKES, Roderick. *Protecting Europe - the EU's response to hybrid threats*. Paris: European Union Institute for Security Studies, Abr.2019. 53 p. Disponível em: <https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_151.pdf>. Acesso em: 22AGO 2020.

FRIEDE, Reis. Guerra Híbrida. Revista Militar Portugal, Lisboa, n. 2601, Out.2018. Disponível em: <https://revistamilitar.pt/artigo/1356>. Acesso em: 07MAR2020.

GLENN, Russell W. *Thoughts on "Hybrid" Conflict*. Small Arms Journal, Fev.2009. Disponível em: <https://smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf>. Acesso em: 08FEV 2020.

GOSU, Armand; MANEA, Octavian. *The Russian Psychological Warfare*. 2015. Disponível em: <http://bsad.roec.biz/portfolio-item/the-russian-psychological-warfare/>. Acesso em: 05JUN 2020.

HR/VP – HIGH REPRESENTATIVE OF THE UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY. *Action Plan on Strategic Communication*. Bruxelas, 2015. Disponível em: <http://archive.eap-csf.eu/assets/files/Action%20PLan.pdf>. Acesso em: 27JUN2020.

HOFFMAN, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, Virginia: Potomac Institute for Policy Studies, Dez/2007. 72 p. Disponível em: <https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf>. Acesso em 01FEV2020.

HOFFMAN, Frank G. *Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges*. PRISM, Washington, DC, v.7, n. 4, p. 30 a 47, Nov/2018. Disponível em: <https://cco.ndu.edu/Portals/96/Documents/prism/prism7_4/181204_Hoffman_PDF.pdf?ver=2018-12-04-161237-307>. Acesso em: 07FEV2020.

JAITNER, Margarita. *Russian Information Warfare: Lessons from Ukraine*. In: GEERS, Keneth. Cyber War in Perspective: Russian Aggression Against Ukraine. Tallinn, Estônia: NATO CCD COE Publications, 2015, cap. 10, p. 87-94. Disponível em: <https://ccdcoe.org/uploads/2018/10/Ch10_CyberWarinPerspective_Jaitner.pdf>. Acesso em: 13GO2020.

JOPLING, Michael. *Countering Russia`s Hybrid Threat: an Update*. Bruxelas: Committee on the Civil Dimension of Security, NATO Parliamentary Assembly, 2018. Disponível em: <https://www.nato-pa.int/download-file?filename=sites/default/files/2018-12/166%20CDS%2018%20E%20fin%20-%20HYBRID%20THREATS%20-%20JOPLING_0.pdf>. Acesso em: 12FEV2020.

KELLY, Alan; PAUL, Christopher. *Decoding Crimea: Pinpointing the influence strategies of modern information warfare*. Riga, Letônia: NATO Strategic Communications Centre of Excellence, 2020. 36 p. Disponível em: <https://stratcomcoe.org/decoding-crimea-pinpointing-influence-strategies-modern-information-warfare>. Acesso em: 18MAR2020

KOFMAN *et al*. *Lessons from Russia's Operations in Crimea and Eastern Ukraine*. Santa Monica, CA: RAND CORPORATION, 2017. 128 p. Disponível em: <https://www.rand.org/pubs/research_reports/RR1498.html>. Acesso em: 26FEV2020.

KURK, Kateryna. *Analyzing the Ground Zero: What Western Countries can Learn From Ukrainian Experience of Combating Russian Disinformation*. Praga: European Values Center for Security Policy, Dez.2017. 25 p. Disponível em: <https://www.kremlinwatch.eu/userfiles/analyzing-the-ground-zero-_15263778496914.pdf>. Acesso em: 15FEV2020.

LANDLER, Mark; GORDON, Michael R. *NATO Chief Warns of Duplicity by Putin on Ukraine.* The New York Times, 8 jul. 2014. Disponível em: <https://www.nytimes.com/2014/07/09/world/europe/nato-chief-warns-of-duplicity-by-putin-on-ukraine.html>. Acesso em: 13AGO2020.

LEAL, Paulo Cesar. *A Guerra Híbrida: Reflexos para o Sistema de Defesa do Brasil*. In: EME, Centro de Estudos Estratégicos, Informe Estratégico, Brasília, n. 06, 2015. Disponível em: <http://www.nee.cms.eb.mil.br/attachments/article/90/IE_06_15_02%20OUT.pdf>. Acesso em: 08FEV2020.

LUCAS, Edward. *Deterrence and "Financial Snap Exercises"*. Washington, DC: Center For European Policy Analysis, 2018. Disponível em: <https://www.cepa.org/deterrence-and-financial>. Acesso em: 24AGO2020.

LUCAS, Edward; POMERANTSEV, Peter. *Winning Information War*. Washington, DC: Center For European Policy Analysis, 2016. Disponível em: <https://li.com/wp-content/uploads/2016/08/winning-the-information-war-full-report-pdf.pdf>. Acesso em: 22 Ago. 2020.

MCCANEY, Kevin. *Russia's Hybrid warfare tactics gain upper hand in Ukraine*. Defense Systems, Mar.2015. Disponível em: <https://defensesystems.com/articles/2015/03/24/russia-hybrid-warfare-ukraine-nato.aspx>. Acesso em: 06 Jun. 2020.

Multinational Capability Development Campaign (MCDC) Countering Hybrid Warfare (CHW) Project. *Countering Hybrid Warfare*. Oslo: Norwegian Institute of International Affairs, 2019. Disponível em: <https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding- hybrid-warfare>. Acesso em: 01 Fev. 2020.

MONAGHAN, Sean. *Countering Hybrid Warfare: Conceptual Foundations and Implications for Defense Forces*. Londres: MCDC Countering Hybrid Warfare Project, Mar.2019. Disponível em:

<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840513/20190401-MCDC_CHW_Information_note_-_Conceptual_Foundations.pdf>. Acesso em: 12 Fev. 2020.

NEMETH, William J. Future War and Chechnya: a Case for Hybrid Warfare. 2002. 100 f. Tese - Naval Postgraduate School, Monterey, California, 2002. Disponível em: <https://core.ac.uk/download/pdf/36699567.pdf>. Acesso em 01 Fev. 2020.

PAUL *et al*. Lessons from Others for Future U.S. Army Operations in and Through the Information Environment: Case Studies. Santa Monica, CA: RAND Corporation, 2018. Disponível em: <https://www.rand.org/pubs/research_reports/RR1925z2.html>. Acesso em: 07 Jun. 2020.

PERRY, Bret. Non-Linear Warfare in Ukraine - The Critical Role of Information Operations and Special Operations. Small Wars Journal, 2015. Disponível em: <https://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera>. Acesso em: 10 Ago. 2020.

PINHO, Alessandro Paiva de. A Guerra Híbrida e os Reflexos para o Exército Brasileiro. In: PADECEM, Rio de Janeiro, v. 8, n. 17, p. 071-083, 02/2016. Disponível em: <http://www.eceme.eb.mil.br/images/docs/Padeceme/PADECEME-2016-2.pdf>. Acesso em: 08FEV2020

POMERANTSEV, Peter; WEISS, Michael. *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. Nova Iorque: Institute of Modern Russia, The Interpreter, 2014. Disponível em: <https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf>. Acesso em: 25 Mar. 2020.

POMERANTSEV, Peter. From ISIS to Russia- How War Changed in 2015. Washington, DC: The Atlantic, 2015. Disponível em: <https://www.theatlantic.com/international/archive/2015/12/war-2015-china-russia-isis/422085/>. Acesso em: 14 Ago. 2020.

RADIN, Andrew. *Hybrid Warfare in the Baltics Threats and Potential Responses*. Santa Monica, CA: RAND Corporation, 2018. Disponível em: <https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf>. Acesso em: 05 Fev. 2020.

REICHBORN-KJENNERUD, Erik; CULLEN, Patrick J. *Understanding Hybrid Warfare*. Oslo: Norwegian Institute of International Affairs, 2016. Disponível em: <https://www.nupi.no/en/Publications/CRIStin-Pub/What-is-Hybrid-Warfare>. Acesso em: 01 Fev. 2020

RUSSIA. Doutrina Militar da Federação Russa. Moscou, 2014. Disponível em: <https://www.rusemb.org.uk/press/2029>. Acesso em: 20 Ago. 2020.

SAZONOV *et al*. *Russian Information Campaign Against Ukrainian State And Defence Forces*. Tartu, Estônia: NATO Strategic Communications Centre of Excellence, 2016. Disponível em: <https://stratcomcoe.org/russian-information-campaign-against-ukrainian-state-and-defence-forces>. Acesso em: 13 Ago. 2020.

SNEGOVAYA, Maria. *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare*. Washington, DC: Institute for the Study of War, 2015. Disponível em: <http://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin%27s%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf>. Acesso em: 13 Jun. 2020.

TREVERTON, Andrew T. et al. *Addressing Hybrid Threats*. Estocolmo: The European Centre of Excellence for Countering Hybrid Threats, 2018. Disponível em: <https://www.hybridcoe.fi/wp-content/uploads/2018/05/Treverton-AddressingHybridThreats.pdf>. Acesso em: 07 Fev. 2020.

WALKER, Robert G. *Spec Fi - The U.S. Marine Corps and Special Operations*. 1998. 111 f. Tese - Naval Postgraduate School, Monterey, California, 1998. Disponível em: <https://apps.dtic.mil/dtic/tr/fulltext/u2/a359694.pdf>. Acesso em: 22 Fev. 2020.

WEITZ, Richard. *Countering Russia's Hybrid Threats*. Estônia: International Centre for Defense and Security, 2014. Disponível em: <https://icds.ee/countering-russias-hybrid-threats/>. Acesso em: 07 Jun. 2020.

WITHER, James K. *Making Sense of Hybrid Warfare*. Connections, Nova Iorque, v. 15, n. 2, p. 73-87, 2016. Disponível em: <https://www.jstor.org/stable/26326441>. Acesso em: 01FEV2020.

APÊNDICE A – GUERRA HÍBRIDA E AMEAÇA HÍBRIDA

À medida que o conceito de Guerra Híbrida foi se disseminando, novos termos relacionados a ele foram surgindo e contribuíram para dificultar sua compreensão. O termo Ameaça Híbrida, em particular, surge com bastante frequência na literatura. Junto com isso, a ampliação do conceito e a relevância dada, em algumas definições, ao emprego de meios não militares o afastaram do entendimento tradicional da guerra e o aproximaram do que muitos consideram ser as relações competitivas e conflituosas entre os Estados. Dessa forma, iremos agora analisar como esses termos estão relacionados.

Para Wither (2016), essa abordagem mais ampla da Guerra Híbrida, que inclui o emprego de uma variedade de meios não militares e onde o agressor procura operar abaixo dos limites de resposta do oponente, se aproxima muito da visão realista da política internacional, onde as relações entre os Estados são naturalmente competitivas e conflituosas. Nesse contexto, na busca pela consecução de seus interesses nacionais, os Estados já fazem uso de todos os instrumentos do poder nacional (WITHER, 2016). Para esse autor, somente quando os meios não militares fossem coordenados ou integrados com a ameaça do uso ou o uso real da força é que essa rivalidade natural daria lugar à Guerra Híbrida (WITHER, 2016).

Já segundo Monaghan (2019), esse conceito se afasta da proposta original de Hoffman, que aborda a mudança no caráter da guerra, onde os atores empregam combinações de suas capacidades para ganhar vantagens assimétricas, e se aproxima do que ele chama de Grande Estratégia não violenta de Estados revisionistas,[116] [117] que procuram obter vantagens enquanto evitam represálias explorando a zona cinza entre guerra e paz. Essa abordagem passou a ser tratada como Ameaça Híbrida,[118] uma vez que as ações do ator híbrido nas zonas cinzas não permitem sua caracterização como "guerra" e removem ou impedem a capacidade do oponente responder decisivamente (MONAGHAN, 2019).

O conceito de Ameaça Híbrida passou a ser abordado em vários documentos, inclusive no estabelecimento de contramedidas, o que contribuiu para que os dois termos e conceitos fossem confundidos. Para Monaghan (2019), essa confusão conceitual dificulta a compreensão da natureza distinta dos desafios e o consequente desenvolvimento de uma

[116] Grande Estratégia é a forma mais complexa de planejamento de um país para se alcançar um objetivo de longo termo. Para isso, o governo tenta desenvolver a melhor maneira possível de coordenar capacidade militar, influência política, habilidade diplomática e poder econômico dentro de uma estratégia nacional coesa (Enciclopédia Britânica).

[117] Estados revisionistas são aqueles que buscam alterar o status quo da distribuição de poder no sistema internacional a seu favor.

[118] Afastando-se da definição original de Hoffman para o termo, que focava em um **adversário** que simultaneamente e adaptativamente emprega uma mistura de armas convencionais, táticas irregulares, terrorismo catastrófico e comportamento criminal, em um campo de batalha para alcançar os objetivos políticos desejados (HOFFMAN, 2007).

estratégia de defesa. Assim, ele propõe a seguinte distinção conceitual:

> Ameaças Híbridas combinam uma ampla gama de meios não violentos para atingir vulnerabilidades em toda a sociedade, a fim de minar o funcionamento, a unidade ou a vontade de seus alvos, enquanto degradam e subvertem o status quo. Esse tipo de estratégia é usado por atores revisionistas para alcançarem gradualmente seus objetivos sem desencadear respostas decisivas, incluindo respostas armadas. A Guerra Híbrida é o desafio apresentado pela crescente complexidade dos conflitos armados, onde os adversários podem combinar tipos de guerra e meios não militares para neutralizar um poder militar convencional. (MONAGHAN, 2019, p. 3, tradução nossa).

Ainda de acordo com Monaghan (2019), outra diferença entre os dois conceitos se refere ao foco principal das ações. Em uma Ameaça Híbrida, o principal alvo é a vontade da população e a capacidade de tomada de decisão do governo, pela atuação nos campos cognitivo e psicológico (MONAGHAN, 2019). Já na Guerra Híbrida, o ator híbrido busca reduzir a efetividade das forças militares conduzirem suas operações com sucesso pela combinação inovadora e eficiente de táticas, meios e recursos (MONAGHAN, 2019).

Assim como Monaghan (2019), Treverton *et al* (2018) também entende que, na Ameaça Híbrida, o objetivo é alcançar resultados sem efetivamente entrar em guerra. Por isso, o alvo das operações são as sociedades como um todo e não apenas seus combatentes. Dessa forma, a distinção entre combatentes e não combatentes é demolida inteiramente. Nesse sentido, o conceito de Ameaça Híbrida se distância do entendimento do que é a guerra, que continua a ocupar um dos extremos do espectro híbrido, mas assume um aspecto muito mais amplo, combinando guerra cinética com operações psicológicas e cibernéticas (TREVERTON *et al*, 2018).

Com base nessa distinção, pode-se observar que as Guerras Híbridas e as Ameaças Híbridas estão em posições diferentes dentro do Continuum dos Conflitos. A FIG. 7 abaixo ilustra essa distribuição:

As Ameaças Híbridas tem uma intensidade menor que a de um conflito de baixa intensidade, uma vez que as ações envolvidas são projetadas para ficar abaixo da percepção de um ato de guerra. Já as Guerras Híbridas é um conflito armado entre a Guerra Irregular e a Guerra convencional, uma vez que se vale de ações de ambos os tipos (MONAGHAN, 2019).

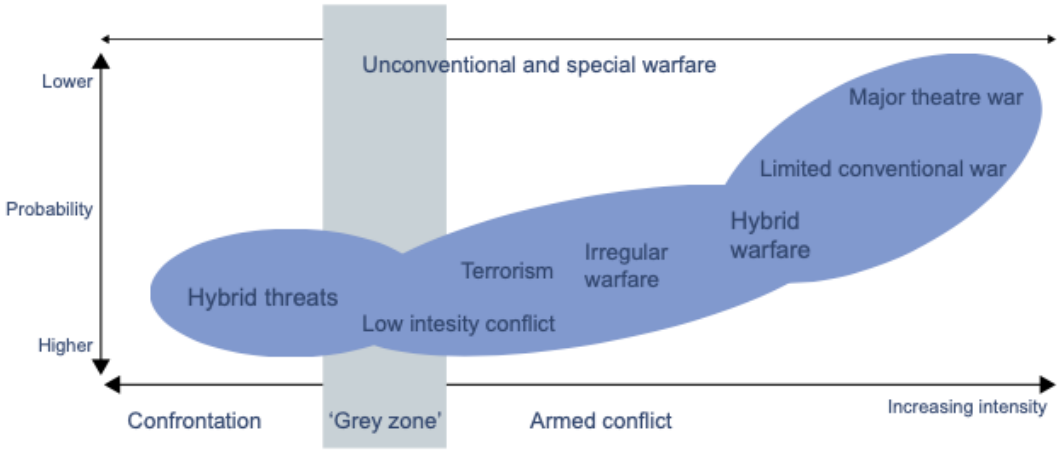

FIGURA 7 – Ameaças Híbridas e Guerras Híbridas no Continuum dos Conflitos
Fonte: MONAGHAN, 2019, p. 4.

Apesar da distinção teórica apontada, a linha que separa a Ameaça Híbrida da Guerra Híbrida é muito tênue. Ambas podem ocorrer simultaneamente, conduzidas pelo mesmo adversário, como parte de uma campanha (MONAGHAN, 2019). Exemplo disso foram as ações da Rússia na Ucrânia, quando, ao mesmo tempo em que empregou pressões econômicas e políticas contra o governo ucraniano, financiou manifestações a favor de seus interesses e promoveu uma intensa campanha de desinformação em diversas mídias (no que se enquadra dentro do conceito de ameaça híbrida, por não poderem ser caracterizadas como ações de guerra), a Rússia empregou tropas regulares para invadir a Criméia, enviou equipamentos e militares de ligação para apoiar rebeldes separatistas no leste da Ucrânia e infiltrou combatentes descaracterizados para combater ao lado destes ("pequenos homens verdes") (ações mais próximas ao entendimento de guerra) (KOFMAN *et al*, 2017).

A distinção proposta por Monaghan, separando os conceitos de acordo com a intensidade das ações dentro do Continuum dos Conflitos, proporciona uma melhor compreensão teórica do fenômeno. Ela posiciona as Ameaças Híbridas na porção menos intensa do espectro, onde os meios não militares são o foco das ações, mas onde a ameaça da força militar está presente e representa um risco potencial. Já a Guerra Híbrida engloba as ações mais próximas ao conceito original de Hoffman (2007), que caracterizam a complexidade dos conflitos contemporâneos, onde os efeitos sinérgicos da combinação de diversos aspectos da guerra e de meios não militares são direcionados para derrotar um oponente.

Por fim, é importante ressaltar que não há um consenso sobre os argumentos apresentados neste item e que muitos documentos que tratam do assunto foram produzidos antes desse estudo. Além disso, apesar das diferenças teóricas apresentadas aqui, a Ameaça e a Guerra Híbrida fazem parte do mesmo fenômeno e as linhas que os separam são muito tênues e podem ser cruzadas a qualquer instante. Dessa forma, para o interesse da presente pesquisa,

consideraremos que ambos os termos tratam de uma ameaça mais ampla, onde todos os instrumentos do poder são empregados contra as vulnerabilidades percebidas de um oponente para a consecução de objetivos políticos.

APÊNDICE B – A INFORMAÇÃO COMO UMA ARMA

Neste anexo, iremos identificar o conceito, as características e as principais ferramentas da Guerra de Informação, de modo a entendermos sua importância e os efeitos gerados pelo seu emprego.

Para Pomerantsev e Weiss (2014), a liberdade de informação e de expressão são fundamentais para uma globalização baseada na liberal democracia, por possibilitar o debate e o bem comum. Mas, o que acontece quando essa liberdade de informação é usada para subverter esses princípios e tornar o debate e o pensamento crítico impossíveis? Se ela for usada não para informar ou persuadir, mas como uma arma? Segundo esses autores, pelo menos desde 2008, a informação tem sido pensada não como uma ferramenta para a persuasão, diplomacia ou mesmo propaganda, mas como uma arma, para confundir, desmoralizar, chantagear, paralisar e subverter (POMERANTSEV; WEISS, 2014).

De acordo com Kelly e Paul (2020), no que se refere à guerra moderna, informação é a nova munição. Ela não é disparada do cano de uma arma, mas seu impacto e efeitos de persuasão são indiscutíveis (KELLY; PAUL, 2020). A transformação da informação em uma arma, chamada de Guerra da Informação, é um elemento chave da Guerra Híbrida (POMERANTSEV; WEISS, 2014). Ao conseguir dominar a "armamentização" da informação,[119] um ator híbrido inclui uma forma de guerra não material e não militar muito mais intensa, reforçando o componente psicológico da guerra (WEISS, 2015).

O uso da informação como uma arma não é algo novo, mas sua sofisticação e intensidade estão aumentando e, somente mais recentemente, o ocidente começou a perceber que a desinformação representa uma séria ameaça (LUCAS; POMERANTSEV, 2016). Assim, embora a Guerra da Informação não seja nova, a urgência em dominá-la é. A doutrina militar russa,[120] por exemplo, reconhece o ambiente informacional como um de seus domínios. A expansão do acesso às mídias sociais, os resultados positivos alcançados com o processamento de "big data" e os avanços resultantes da inteligência artificial romperam as abordagens tradicionais do seu emprego (KELLY; PAUL, 2020).

Operações de informação envolvem uma mistura de propaganda, desinformação e manipulação da mídia para confundir e dividir a opinião no Estado alvo, explorando quaisquer divisões dentro da sociedade, sejam políticas, econômicas, étnicas e sociais (WEITZ, 2014) e criando um poderoso componente psicológico no conflito (GOSU; MANEA, 2015). Segundo

[119] Do original *weaponization of information*, tradução nossa.
[120] Doutrina Militar da Federação Russa, 2014. Disponível em: https://www.rusemb.org.uk/press/2029.

Lucas e Pomerantsev (2016), os modernos métodos da Guerra da Informação são ajustados para confundir, desorientar e distrair. Ela explora tensões étnicas, linguísticas, sociais e históricas e promove causas contrárias ao sistema em vigor, ampliando seu alcance e dando a elas uma falsa aparência de legitimidade (LUCAS; POMERANTSEV, 2016).

Para Vadimir Pirumov,[121] a Guerra da Informação consiste em:

> "[...] garantir os objetivos da política nacional, tanto na paz quanto na guerra, por meio de técnicas e meios para influenciar as fontes de informação do lado oposto.... e inclui influenciar o sistema de informações e a condição psíquica". As técnicas de influência da informação incluem "desinformação (decepção), manipulação (de uma situação ou de uma sociedade), propaganda (conversão, separação, desmoralização, deserção, cativar), fazer lobby, controle de crise e chantagem. (PIRUMOV, 2010 *apud* POMERANTSEV; WEISS, 2014, p12, tradução nossa).[122]

A Guerra da Informação pode se valer de várias ferramentas. Para Lucas e Pomerantsev (2016), essas ferramentas incluem os canais de propaganda abertos, como redes de rádio e televisão, *proxies* disfarçados de meios de comunicação convencionais e mídias sociais. Conforme citado anteriormente, a exploração das novas plataformas de mídia ampliou o potencial da Guerra da Informação dentro da Guerra Híbrida.

Enquanto, antigamente, a Guerra da Informação dependia da mídia tradicional, ela agora incorporou o ambiente digital (LUCAS; POMERANTSEV, 2016). Ela explora o anonimato, a ambiguidade, a onipresença e a flexibilidade da internet, em particular as mídias sociais (LUCAS; POMERANTSEV, 2016). Para isso, ela faz uso de *bots* (contas automáticas), *trolls* e websites ou contas de mídia social falsas, que imitam as verdadeiras para semear confusão (LUCAS; POMERANTSEV, 2016). De acordo com Pomerantsev e Weiss (2014), teóricos russos consideram a internet, a comunicação móvel e as mídias sociais fatores decisivos na transformação da informação em uma arma.

Assim como as ações da Rússia na Ucrânia trouxeram uma nova perspectiva ao conceito da Guerra Híbrida, elas também mostraram como a Guerra de Informação moderna pode contribuir, dentro do espectro mais amplo da Guerra Híbrida, para a consecução dos objetivos políticos e estratégicos. O uso da Guerra da Informação pelo Governo russo se baseia na desinformação e seu objetivo não é convencer ou persuadir, mas enfraquecer a vontade das pessoas, mantendo-as distraídas e passivas (LUCAS; POMERANTSEV, 2016).

A desinformação é empregada para desorganizar e desmoralizar um oponente e é travada no domínio da percepção e da mente das pessoas (LUCAS; POMERANTSEV, 2016).

---

[121] Antigo chefe da Diretoria de Guerra Eletrônica do Estado-Maior Naval russo (do original *Directorate for Eletronic Warfare of the Main Naval Staff*, tradução nossa).

[122] PIRUMOV, VADIMIR S. "Informatsionnoe Protivoborstvo. 3". Moscow, 2010.

Ela se vale de uma técnica chamada controle reflexivo,[123] que procura induzir o adversário a voluntariamente adotar ações mais vantajosas aos objetivos russos, moldando sua percepção (SNEGOVAYA, 2015). De acordo com Lucas e Pomerantsev (2016), o conceito do controle reflexivo é levar o inimigo a se autodestruir, encontrando, enfatizando e explorando um elo fraco entre os conceitos, conhecimentos, ideias e experiências que são a base do seu processo decisório. Foi assim que a Rússia levou os EUA e a UE a permanecerem passivos diante de seus esforços para desestruturar e desmantelar a Ucrânia (SNEGOVAYA, 2015).

Diante do exposto, percebe-se que a evolução dos meios de comunicação tem tornado cada vez mais eficaz o emprego da informação como uma arma. Embora não seja algo novo, a Guerra da Informação vem sendo empregada com maior sofisticação e intensidade. As ações da Rússia na Ucrânia foram um exemplo da contribuição que a Guerra da Informação pode dar dentro da estratégia mais ampla da Guerra Híbrida. Nesse contexto, a desinformação é uma ferramenta importante para moldar a percepção dos envolvidos.

[123] Controle reflexivo é definido como um meio de transmitir a um parceiro ou oponente informações especialmente preparadas para incliná-lo a, voluntariamente, tomar a decisão predeterminada desejada pelo iniciador da ação (THOMAS, 2004). Timothy L. Thomas, "Russia's Reflexive Control Theory And The Military," Journal Of Slavic Military Studies 2004, 17: 237–256, https://www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf.

APÊNDICE C – ESTABELECENDO OBJETIVOS ESTRATÉGICOS E LIMITES PARA RESPOSTA

Diante da ameaça ou da possibilidade de um ataque híbrido, faz-se necessário decidir que postura adotar. Essa decisão, obviamente, dependerá do contexto e de suas variáveis, como as capacidades disponíveis ao Estado atacado para lidar com a situação, o apoio do público interno, as relações com o agressor, a intensidade da ameaça e o ambiente político internacional (MCDC, 2019).

Uma vez que a resposta a ser adotada será uma decisão política, o modelo estudado propõe que sejam estabelecidos objetivos estratégicos para articular e nortear as ações a serem adotadas, que deverão contribuir para a consecução do objetivo definido. Três objetivos estratégicos genéricos foram identificados no estudo para serem empregados na formulação de estratégias de combate à Guerra Híbrida:

a) Manter a capacidade governamental de realizar ações independentes, combatendo os efeitos da Guerra Híbrida sobre o funcionamento básico do governo e da sociedade. Envolve o desenvolvimento da resiliência nas funções críticas da sociedade (PMESII),[124] avaliando e minimizando suas vulnerabilidades (MCDC, 2019)

b) Dissuadir possível agressores de realizarem ataques híbridos, seja demonstrando a capacidade de resistir a esses ataques, impedindo o agressor de atingir o efeito desejado, seja pela ameaça de uma resposta que tornaria o efeito resultante desvantajoso para o agressor (MCDC, 2019); e

c) Impedir que um adversário seja capaz de realizar outras agressões híbridas, pela adoção de medidas para prejudicar ou degradar sua capacidade de ação (MCDC, 2019).

O objetivo estratégico deve ser estabelecido desde o início de uma campanha de combate à Guerra Híbrida e pode ser alterado a qualquer momento, mediante reavaliações da situação, das capacidades disponíveis, das ações do agressor e dos efeitos alcançados com as ações já adotadas. Tanto na definição inicial, quanto nas avaliações subsequentes dos objetivos estratégicos, os limites para resposta estabelecidos serão uma referência importante para a tomada de decisão. Veremos a seguir algumas considerações sobre essa questão.

Os limites para resposta são estabelecidos para orientar os decisores quanto ao momento de adotar ações em resposta a um ataque híbrido. Como é muito difícil interpretar quando uma ação faz parte das relações normais entre os atores do sistema internacional e

[124] Organizadas, nesse estudo, nos campos político, militar, econômico, social, informacional e de infraestrutura (PMESII) (MCDC, 2019).

quando elas fazem parte de ataque híbrido, os limites para resposta são fundamentais no estabelecimento dos objetivos estratégicos, pois definem qual o nível de hostilidade será tolerado e qual irá requerer uma resposta (MCDC, 2019).

Devem ser estabelecidos limites para resposta para todas as funções críticas da sociedade. Contudo, é fundamental que sua análise seja feita de maneira integrada, de modo a permitir a compreensão do quadro completo da ameaça, devido à natureza sinérgica dos ataques na Guerra Híbrida (MCDC, 2019). Outro aspecto importante a ser considerado é se esses limites serão comunicados ou não, visto que seu conhecimento poderá ser útil para que um agressor híbrido ajuste a intensidade de suas ações, no que já foi caracterizado como escalada vertical da Guerra Híbrida (MCDC, 2019).

Dessa forma, com base nas informações apresentadas, depreende-se que o estabelecimento dos limites para resposta deve ser feito com o auxílio de peritos nas respectivas áreas em que serão empregados. Esses peritos deverão levar em consideração parâmetros relativos a níveis normais de atividade em cada uma dessas áreas e propor índices de referência que indiquem uma atitude agressiva. Contudo, caberá ao nível político, em conjunto com os objetivos estratégicos, definir o limite de tolerância para esse ataque.

Entretanto, para que os limites de resposta possam ser empregados, é necessário, primeiramente, conseguir identificar o ataque híbrido. Assim, o modelo apresentado tem sua primeira componente centrada no desenvolvimento da capacidade de detecção, como será visto a seguir.

APÊNDICE D – AÇÕES PARA DISSUADIR AGRESSORES HÍBRIDOS

O estudo realizado pelo MCDC apresenta medidas que podem ser aplicadas às funções críticas da sociedade, organizadas nos domínios PMESII, para aumentar a resiliência e minimizar os efeitos de ataques híbridos (MCDC, 2019). Essa abordagem está focada na dissuasão por negação, por considerar que, por envolver ações direcionadas contra um eventual agressor, a dissuasão por punição, dentro do modelo do combate à Guerra Híbrida proposto pelo MCDC, se enquadra melhor dentro do componente de resposta a ataques híbrido, que será analisado mais à frente (MCDC, 2019). O QUADRO 2 abaixo traz exemplos de medidas que podem ser adotadas dentro de cada área dentro do espectro das vulnerabilidades críticas da sociedade:

QUADRO 2

Exemplos de medidas para dissuasão

Espectro das vulnerabilidades nacionais (PMESII)	MEDIDAS
POLÍTICO	- Restringir ou proibir o financiamento externo de partidos políticos ou organizações afiliadas a partidos políticos; e - Proteção aos processos eleitorais.
MILITAR	- Manter um poder militar crível; - Desenvolver a cooperação internacional para a defesa; - Planejar a força considerando as ameaças híbridas modernas; e - Desenvolver a resiliência do setor de defesa.
ECONÔMICO	- Aprimorar a segurança e buscar fontes diversas para os recursos estratégicos; - Aumentar a consciência situacional das empresas privadas sobre as ameaças híbridas; e - Combater a corrupção.
SOCIAL	- Adotar medidas para reduzir a exploração de divisões sociais, combatendo o financiamento e o apoio externos; - Desenvolver campanhas para educação da população, de modo a melhorar a compreensão sobre a existência e as formas de atuação das ameaças híbridas e sobre as medidas que devem ser adotadas; e - Conduzir campanhas de comunicação estratégica para envolver a população no fortalecimento da resiliência.
INFRAESTRUTURA	- Desenvolver medidas para proteção física da infraestrutura crítica; e - Atualizar normas, regulamentos e regras que possam conter brechas que venham a ser exploradas por um agressor híbrido; e

	- Adotar procedimentos para aumentar a transparência das transações financeiras.
INFORMAÇÃO	- Aprimorar a comunicação estratégica, tanto interna quanto externa; e - Buscar a cooperação da mídia tradicional e digital.

Fonte: MCDC, 2019, p. 45 e 46.

As ações propostas na tabela acima foram elaboradas com base em diversos estudos conduzidos pelos analistas vinculados ao MCDC, em estudos de caso e em iniciativas já adotadas por governos e instituições na Europa e buscam apenas prover exemplos que ilustrem a abordagem do modelo desenvolvido. Novamente, para traçar um paralelo com esse modelo, será abordada como a questão da dissuasão é tratada na estratégia da UE contra a Guerra Híbrida.

APÊNDICE E – AÇÕES PARA RESPONDER A ATAQUES HÍBRIDOS

Assim como no caso da dissuasão, o estudo realizado pelo MCDC apresenta exemplos e considerações sobre como as expressões do poder podem ser empregadas em resposta a ameaças híbridas. É interessante observar que, em comparação com os exemplos apresentados para a dissuasão, os exemplos são bem mais limitados, como pode ser observado no QUADRO 3, abaixo.

QUADRO 3

Exemplos de medidas para resposta

Expressões do Poder (MPECI)	MEDIDAS
MILITAR	- A resposta deve garantir proporcionalidade em relação a agressão; - Deve maximizar o potencial coercitivo; - Deve ser direcionado às vulnerabilidades do agressor; e - Deve estar alinhado com objetivo estratégico.
POLÍTICO	- Restrições de viagem a representantes políticos; - Expulsão de diplomatas; - Suspensão da participação de Estados em organizações internacionais; e - Retirada do direito ao voto nessas organizações.
ECONÔMICO	-Sanções e punições econômicas a Estados e indivíduos.
CIVIL	- Processos criminais; e - Acusação pública.
INFORMAÇÃO	- Apoiar a abertura e transparência da Mídia; - Combater a desinformação por meio da educação e ações legais; e - Empregar medidas cibernéticas ofensivas.

Fonte: MCDC, 2019, p. 58.

ANEXO A – VARIEDADE DE FERRAMENTAS HÍBRIDAS

QUADRO 4
Variedade de Ferramentas Híbridas

FERRAMENTAS DAS AMEAÇAS HÍBRIDAS		
Propaganda	Meios de comunicação domésticos	Financiamento a organizações
“Fake News”	Mídias sociais	Vazamentos estratégicos
Partidos políticos	Protestos organizados	Oligarquias
Ferramentas cibernéticas	Proxies	Guerra não reconhecida
Organizações paramilitares	Influência Econômica	

Fonte: TREVERTON *et al*, 2018, p. 45 a 59.

ANEXO B – INSTRUMENTOS MILITARES E NÃO MILITARES DA GUERRA HÍBRIDA

QUADRO 5

Instrumentos militares da Guerra Híbrida[125]

TIPOS DE INSTRUMENTOS MILITARES (POTENCIAIS TIPOS DE GUERRA)		
Guerra convencional (4)	Guerra irregular (4)	Terrorismo (4)
Criminalidade (larga escala) (4)	Guerra de informação (5)	Guerra nuclear (1)
Guerra biológica/química (1)	Guerra ecológica (1)	Guerra espacial (1)
Guerra eletrônica (1)	Guerra de concussão (1)	Guerra em rede (1)
Guerra de inteligência (1)	Guerra cibernética (6)	Guerra urbana (6)
Guerra não tripulada (6)		

Fonte: MONAGHAN, 2019, p. 7

QUADRO 6

Instrumentos não militares da Guerra Híbrida

TIPOS DE INSTRUMENTOS NÃO MILITARES		
Cultural (1)	Diplomático (1)	Redes (1)
Inteligência (1)	Psicológico (1)	Tecnológico (1)
Contrabando (1)	Guerra das Drogas (1)	Guerra Fictícia ou fabricada (1)
Financeiro (1)	Comércio (1)	Recursos (1)
Econômico/Incentivos econômicos (1)	Legal/Moral/regulatório (1)	Deslocamentos/migração populacional forçada (1)
Mídia/propaganda (1)	Ideológico/religião (1)	Sanções (1)
Meios sigilosos (2)	Guerra não convencional (2)	Guerra de Proxy (2)
Redes Domésticas (3)	Coerção militar (abaixo da guerra) (3)	

Fonte: MONAGHAN, 2019, p. 5.

[125] As fontes para definição desses instrumentos, identificadas pelos números entre parênteses na tabela, foram as seguintes: (1) Liang and Xiangsui's trans-military and non-military forms of warfare in Unrestricted Warfare (1999); (2) RAND study, Modern Political Warfare (2018); (3) Dubik and Vincent, America's Global Competitions: The Gray Zone in Context, ISW (2018); (4) Frank Hoffman's original definition of hybrid warfare (See for example Frank G Hoffman, Hybrid Threats, 2009); (5) Mattis and Hoffman's 2005 definition of the 'four block war' (Mattis and Hoffman, Hybrid War, 2005); e (6) The UK Future Force Concept (2017) .

ANEXO C – CANAIS MAIS IMPORTANTES PARA A DESINFORMAÇÃO RUSSA

QUADRO 7
Canais mais importantes para a desinformação russa

CANAL	EXEMPLOS
Canais de televisão nacionais russos	LifeNews, Россия1, Россия24, Первый канал, НТВ, РЕН ТВ.
Canais de TV ucranianos	Inter e Ukraina24
Mídia online tradicional	Komsomolskaya Pravda v Ucrânia, Regnum e TV Zvezda
Mídias Sociais	Facebook, Twitter, Odnoklassniki, Vkontakte (Vk.com), LiveJournal (livejournal. Com), Liveinternet (li.ru), YouTube, RuTube
Jornais pró-russos da Ucrânia	Vesti, de Kiev
Websites	Новости Донецкой Республики202 e Центральное информационное агентство Новороссиии203
Canais de rádio russos	Radio Mayak
Operadoras de telefonia móvel	KyivStar e MTS (MTC)
Alto-falantes e reprodutores de mídia	usados para influenciar a moral dos soldados ucranianos

Fonte: SAZONOV et al, 2016, p. 102.

ANEXO D – PRINCIPAIS TEMAS EMPREGADOS NA CAMPANHA DE DESINFORMAÇÃO RUSSA

QUADRO 8
Principais temas empregados na campanha de desinformação russa

CRIMÉIA	
A aquisição da Criméia pela Ucrânia foi um erro histórico.	As etnias russas e a população que fala russo na Criméia estão sob severa ameaça ultranacionalista.
A Rússia não estava envolvida nos eventos na Criméia.	Soldados no Criméia voluntariamente se aliaram à Rússia.
REVOLUÇÃO MAIDAN	
Yanukovych fugiu devido a um violento golpe de estado. O novo governo é ilegítimo.	A Revolução Maidan é fascista, nacionalista e antissemita.
A maioria dos protestantes eram violentos ultranacionalistas contrários à Rússia.	Centenas de milhares de russos fugiram da Ucrânia com medo por suas vidas.
DIFAMAR A UCRÂNIA COMO UM ESTADO	
A Ucrânia é um Estado economicamente falido.	A Ucrânia não tem um futuro viável sem os subsídios ou o patrocínio russos.
O governo ucraniano está cheio de ultranacionalistas violentos.	A população pró-europeia é ideologicamente descendente de apoiadores de nazistas e fascista.

Fonte: KOFMAN et al, 2017, p. 79 e 80.