GUERRA HÍBRIDA

Capitão-Tenente ARTUR **KREPP** LISBOA
Encarregado da Divisão de Armamento do DIAsA – CAAML
Aperfeiçoado em Armamento

> Guerras não são mais declaradas, e tendo começado, ocorrem sob uma nova perspectiva. O papel dos meios não militares para atingir objetivos políticos e estratégicos tem aumentado, e em muitos casos, eles excedem a efetividade do armamento. O foco dos métodos aplicados nos conflitos foi alterado para o amplo uso de medidas políticas, econômicas, informacionais, humanitárias e outras medidas não militares, aplicadas em coordenação com a potencial instabilidade da população local. (GERASIMOV, 2016)

INTRODUÇÃO

Conceitos como assimétrico, irregular, não convencional e híbrido são, geralmente, utilizados em discussões políticas e acadêmicas para descrever a complexidade e as características dos conflitos modernos, em que ambos os atores, estatais e não estatais, combinam métodos convencionais com métodos que estão fora do entendimento tradicional das operações militares.

A conceituação de guerra híbrida ganhou maior relevância no cenário mundial após as operações da Rússia na Crimeia e no Leste da Ucrânia em 2014, onde os esforços não eram concentrados apenas no Teatro de Operações. Na verdade, a maior ênfase foi nos métodos não militares que mitigaram a necessidade de um conflito armado.

Mas afinal, o que é guerra híbrida?

A *Multinational Capability Development Campaign* (MCDC), iniciativa multinacional da Organização do Tratado do Atlântico Norte (OTAN), definiu guerra híbrida como sendo o uso sincronizado de múltiplos instrumentos de poder personalizados a vulnerabilidades específicas por meio do amplo espectro das funções sociais, de forma a obter efeitos sinérgicos. Simplificando, a guerra híbrida utiliza atividades sincronizadas de modo a explorar as vulnerabilidades nos campos político, militar, econômico, social, informacional e de infraestrutura, criando efeitos lineares e não lineares.

Jan Joel Andersson (2015), analista sênior do Instituto de Estudos de Segurança da União Europeia, caracterizou guerra híbrida como uma forma de guerra que utiliza um conjunto de métodos, convencionais e não convencionais, militares e não militares, ações ostensivas ou encobertas envolvendo guerra cibernética e informacional com o propósito de gerar confusão e ambiguidade na natureza, origem e objetivo dessas ações.

A relativa novidade da Guerra Híbrida reside na habilidade de um ator em sincronizar múltiplos instrumentos de poder simultaneamente e, intencionalmente, explorar a criatividade, imprecisão, não linearidade e os elementos cognitivos da guerra. Normalmente, é adaptada de forma a permanecer encoberta da detecção óbvia contando, por vezes, com a velocidade, volume e ubiquidade da tecnologia digital que caracteriza a presente era da informação.

FOTO: HDQwalls.com / Marinha do Brasil
Composição Fotográfica: 1ºSG Severiano

A ambiguidade é usada na Guerra Híbrida para esconder as intenções por trás das ações do ator envolvido, dificultando o processo de tomada de decisão do oponente e posterior adoção de uma resposta adequada. Para que isso ocorra, as ações são planejadas de forma a permanecer abaixo da percepção do que caracterizaria um ato de guerra, de modo a tornar ilegítima (ou, pelo menos, politicamente irracional) uma resposta militar.

GUERRA HÍBRIDA RUSSA

A abordagem contemporânea da Rússia é caracterizada pelo uso intensivo do campo informacional, de forças não convencionais, forças convencionais, operações cibernéticas, operações de guerra eletrônica e de grupos paramilitares para atingir objetivos militares alinhados às suas aspirações políticas. Sistematicamente, o emprego de outros instrumentos do Poder Nacional na busca dos objetivos políticos vem crescendo e indo além do uso exclusivo das Forças Armadas.

De forma geral, utilizam ferramentas não militares para reduzirem sua exposição ao escrutínio político e jurídico internacional, com intuito de moldar a narrativa dentro do contexto da guerra de informação/psicológica. A Guerra Híbrida tem como principais características o uso econômico da força, em que busca minimizar o uso tradicional da força militar. É persistente, quebrando a binaridade entre guerra ou paz. Está sempre em prática; a guerra não é declarada, as ações ocorrem em tempos de paz e com variação de intensidade. É centrada na população, influenciando-a por meio de operações de informação e grupos civis locais.

Entre seus objetivos, estão a captura de territórios sem o uso da força, como no caso da Crimeia, a partir da criação de pretextos para o uso convencional da força e influenciando os políticos e as políticas dos territórios além das fronteiras. A Rússia emprega 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 dos Estados.

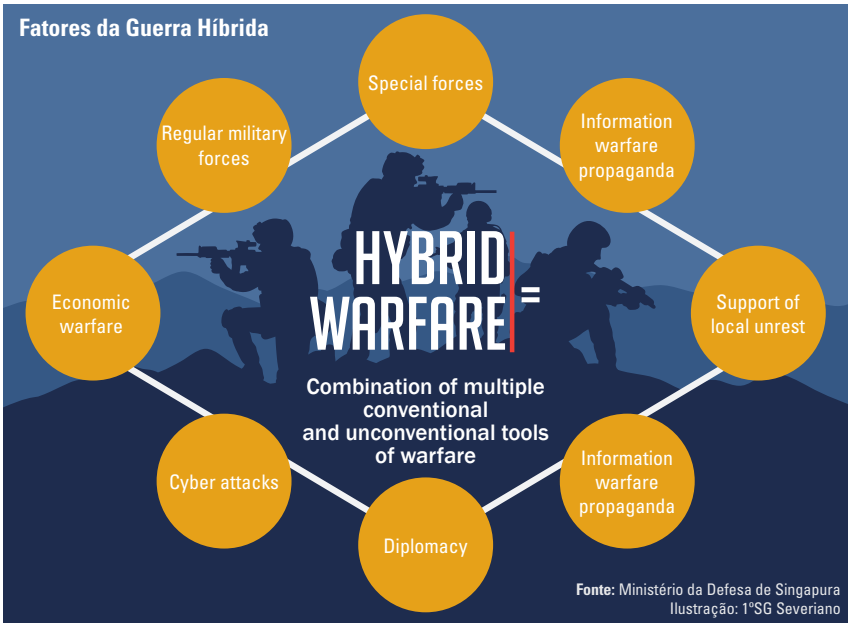
No contexto russo, grande é a relevância do emprego de operações de informação na intenção de moldar as narrativas, utilizando, para isso, recursos de mídia, programas de televisão, patrocínio a pensadores e influenciadores para promover seus ideais, não obstante ataques cibernéticos, grupos paramilitares, influência econômica, medidas clandestinas e influência política. Guerreiros cibernéticos invadem sistemas de informação estrangeiros coletando valiosas informações. Além da obtenção de segredos, utiliza artifícios para direta ou indiretamente manipular sistemas de informação, dos quais o processo político depende.

AS MÍDIAS SOCIAIS NA GUERRA HÍBRIDA

A exploração das novas plataformas de mídia para a condução da Guerra de Informação (GI) 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, caracterizando uma mudança significativa no caráter do conflito moderno. 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 GI vem sendo empregada com maior sofisticação e intensidade. É necessário reconhecer que as campanhas de desinformação modernas foram potencializadas pelas novas tecnologias e aplicativos, como smartphones e mídias sociais. Tais recursos podem ser usados para disseminar a desinformação em larga escala e com uma velocidade e precisão sem precedentes. A internet aumentou grandemente o volume e a variedade de notícias disponíveis e mudou profundamente a maneira como as pessoas, os mais jovens em particular, acessam as notícias.

O ambiente em que vivemos vem mudando drasticamente com o rápido desenvolvimento da tecnologia. Hoje, com o potencial das mídias sociais, todos podemos ser uma fonte de informação capaz de alcançar milhões. A mídia tradicional não é mais o principal ator no espaço informacional.



Fonte: Ministério da Defesa de Singapura
Ilustração: 1ºSG Severiano

Tal fato traz diversos efeitos positivos, mas também, da mesma maneira, muitos negativos. As mídias sociais podem expor diversas vulnerabilidades de seus usuários. O ambiente virtual é desregulado e, por vezes, anônimo, propiciando a oportunidade ideal para a disseminação de visões extremas e desinformação deliberada. Com cada vez mais pessoas conectadas, o medo e as informações falsas se espalham rapidamente, gerando pânico.

Os recentes conflitos demonstram que as mídias sociais têm sido utilizadas como um eficiente instrumento de poder do campo informacional, atacando as vulnerabilidades de diversas formas: identificação nas redes de possíveis alvos e objetivos, coleta de informações de inteligência, invasão de perfis para disseminação de desinformação, influência psicológica e manipulação. Tais usos tendem a ser cada vez mais sofisticados e imprevisíveis, acompanhando as inovações e avanços do ambiente informacional e cibernético.

CONSIDERAÇÕES FINAIS

Os recentes ataques cibernéticos a áreas de infraestrutura, incertezas acerca da possibilidade de intervenção em eleições de outras nações e campanhas de desinformação espalhadas ao redor do globo demonstram os danos que a guerra híbrida pode alcançar sem uma maior escalada da crise. Equiparar-se ao desafio imposto pela complexidade da guerra híbrida levará tempo e esforço, mas, como ponto de partida, é essencial uma coordenação e cooperação interagências para prover melhor detecção das ameaças híbridas e coordenar a reação apropriada.

A sociedade como um todo também precisa estar preparada para lidar com os ataques híbridos, em particular, aqueles direcionados ao 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 a regulação das tensões e insatisfações dentro da sociedade, observando tudo aquilo que tenha potencial de ser explorado em uma campanha de desinformação. Outro aspecto seria 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. E, ainda, identificar e tornar público as pessoas ou grupos defensores de ideologias que estejam sob a influência de agentes externos, permitindo à população compreender as reais motivações por trás de suas ações, enfraquecendo o apoio à desinformação.

Como destacado pela European Values Think Tank, outro aspecto importante refere-se à resiliência dentro das Forças Armadas e das forças de segurança internas. Campanhas de desinformação podem ser empregadas para enfraquecer as lideranças militares perante suas tropas, diminuindo a credibilidade das forças de segurança junto à população e a própria confiança das tropas em sua capacidade de combater o agressor. Assim, o monitoramento diuturno por potenciais ameaças, o acompanhamento constante da moral das tripulações por meio de pesquisas de satisfação e o esforço regular na disseminação do conhecimento sobre a desinformação são medidas que devem ser implementadas.

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, aumentando a consciência situacional, e não dando margem a interpretações maliciosas que possam ser exploradas por agressores híbridos.

Em que pese toda a ambiguidade que a envolve, a Guerra Híbrida já é dominante e largamente difundida, utilizada por atores estatais e não estatais, e provavelmente crescerá como um desafio, justificando novos esforços das nações em entender a ameaça que representa.

Assim, os governos devem estabelecer um processo que vise liderar e coordenar uma abordagem nacional de autoavaliação de suas vulnerabilidades nos diversos campos de análise das possíveis ameaças e das reações adequadas. Esse processo deve direcionar os esforços de todos os setores em entender, detectar e responder às ameaças híbridas.

REFERÊNCIAS:

ANDERSSON, Jan J. Hybrid: what's in a name?. **European Union Institute for Security Studies**, 2015. Disponível em: https://www.iss.europa.eu/content/hybrid-what%E2%80%99s-name. Acesso em: 7 abr. 2021.

GERASIMOV, Valery. The value of science is in the foresight: new challenges demand rethinking forms and methods of carrying out combat operations. **Military Review**, Leavenworth, v. 96, n. 1, 2016. Disponível em: https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf. Acesso em: 16 abr. 2021.

JANDA, Jakub. **Full-scale democratic response to hostile disinformation operations**: 50 measures to oust Kremlin hostile disinformation influence out of Europe. Praga: European Values, 2016. Disponível em: https://www.kremlinwatch.eu/userfiles/full-scale-democratic-response-to-hostile-disinformation-operations.pdf. Acesso em: 16 abr. 2021.

MULTINATIONAL CAPABILITY DEVELOPMENT CAMPAIGN (MCDC). **Countering hybrid warfare project**. Oslo: Norwegian Institute of InternationalAffairs, 2019. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf. Acesso em: 4 abr. 2021.

MULTINATIONAL CAPABILITY DEVELOPMENT CAMPAIGN (MCDC). **Understanding hybrid warfare**. Oslo: Norwegian Institute of InternationalAffairs, 2017. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf. Acesso em: 5 abr. 2021.

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE. **Social Media as a tool of hybrid warfare**. Letônia: NATO Strategic Communications Centre of Excellence, 2016. Disponível em: https://stratcomcoe.org/pdfjs/?file=/cuploads/pfiles/public_report_social_media_hybrid_warfare_22-07-2016-1.pdf?zoom=page-fit. Acesso em: 7 abr. 2021.