ESTUDO DE CASO: INTEGRAÇÃO DA GUERRA ELETRÔNICA, CIBERNÉTICA E ESPACIAL

Análise da Operação Absolute Resolve: como a convergência cibernética, eletrônica e espacial redefine a guerra de precisão e oferece lições cruciais para a defesa e contrainteligência do Brasil no século XXI.

Carlos A. Klomfahs*

Imagem meramente ilustrativa, gerada por inteligência artificial.

"Si vis pacem, para bellum" ("Se queres paz, prepara-te para a guerra") – Publius Flavius Vegetius Renatus, em "De re militari" ("Sobre Assuntos Militares").

Este artigo analisa genericamente a Operação "Absolute Resolve", conduzida pelas Forças de Operações Especiais (SOF) dos EUA em 3 de janeiro de 2026, como um estudo de caso paradigmático de Operações Multidomínio (MDO, *Multi Domain Operations*). O estudo detalha como a convergência de capacidades cibernéticas, eletrônicas e espaciais permitiu a captura cirúrgica de alvos de alto valor (HVT, *High Value Target*) em Caracas, Venezuela, sem baixas aliadas. Através de um *design* de pesquisa focado na doutrina militar contemporânea, o artigo discute a

neutralização de Sistemas de Defesa Aérea Integrada (IADS, *Integrated Air Defense Systems*) por meio de "corredores cibernéticos", o uso de geointeligência (GEOINT) e a inovação no uso da força policial como instrumento de poder militar.

Conclui-se que a operação inaugura uma nova era de guerra de precisão, onde a superioridade informacional precede e viabiliza a ação direta com lições primordiais para o Brasil.

INTRODUÇÃO: UM NOVO PARADIGMA AMERICANO

Nas primeiras horas de 3 de janeiro de 2026, a Operação Absolute Resolve redefiniu os limites das operações especiais modernas. A captura de Nicolás Maduro e Cilia Flores no Complexo Militar de Forte Tiuna não foi apenas um triunfo tático de ação direta, mas o resultado de uma orquestração sem precedentes entre os domínios espacial, cibernético e eletrônico. Este evento marca a transição definitiva para a Guerra de Mosaico, onde a destruição total do inimigo é substituída pela desarticulação funcional de seus sistemas de comando e controle (C2).

Segundo a doutrina de operações conjuntas do Ministério da Defesa, as ações de comando compreendem a captura de pessoas ou bens, sendo portanto, uma ação direta com base em nossa doutrina.

Em nossa consultoria de inteligência, estas ações de forças especiais fornecem elementos cruciais para o planejamento de contrainteligência para empresas e governos, daí nosso interesse em dedicar tempo e publicar apenas o que pode ser publicado.

METODOLOGIA (*DESIGN* DE PESQUISA)

O artigo utiliza um *design* de Estudo de Caso Analítico-Doutrinário, estruturado em três partes:

a) Análise de Integração Multidomínio (MDO): Avaliação de como os domínios espacial e cibernético criaram as condições para a manobra terrestre.

b) Revisão de Doutrina: Aplicação dos conceitos de "corredores de superioridade" e "supressão cibernética de defesas aéreas" (C-SEAD, *Counter-Suppression of Enemy Air Defenses*, ou Contra-Supressão das Defesas Aéreas Inimigas).

c) Análise SWOT da Operação: Mapeamento das forças e vulnerabilidades do modelo executado.

TRIANGULAÇÃO ESPAÇO, CIBERNÉTICA E ELETRÔNICA

Pelo que é possível deduzir de vídeos e reportagens de fontes abertas, a operação americana com forças especiais foi viabilizada pela sincronização de três pilares tecnológicos e de inteligência:

Domínio Espacial e Geointeligência (GEOINT): É fora de dúvida que o uso antecipado de inteligência satelital permitiu o mapeamento meticuloso do "padrão de vida" dos alvos. O emprego de drones de alta altitude, como o RQ-170 Sentinel, forneceu vigilância e reconhecimento (ISR, *Intelligence, Surveillance, Reconnaissance*) persistentes, enquanto a geointeligência transformou a geografia montanhosa de Caracas em uma vantagem tática para a infiltração de helicópteros americanos, de forma precisa e abaixo dos radares.

Guerra Cibernética e "Cegueira" de Radares: Pelo que se infere, a doutrina americana aplicada não buscou somente a destruição física dos radares venezuelanos, mas a criação de corredores cibernéticos. Operações multidomínio altamente sofisticadas "desabilitaram" os radares e neutralizaram as defesas antiaéreas por meio de injeção de dados e negação de serviço (DDoS). Este método permitiu que as aeronaves de assalto entrassem no espaço aéreo soberano sem disparar alertas nos sistemas IADS.

Inteligência de Campo e Infiltração Técnica: Outro ponto operacional observado que se pode presumir é a colaboração entre a CIA e informantes locais foi crucial para a implantação de localizadores de precisão extrema como um suposto relógio ganho de alguém de confiança de Maduro. Estes dispositivos, capazes de operar em ambientes de alta blindagem (*bunkers*), garantiram que a localização do alvo fosse conhecida em tempo real, superando barreiras físicas que impedem ondas de rádio convencionais.

ANÁLISE SWOT (FORÇAS, FRAQUEZAS, OPORTUNIDADES E AMEAÇAS)

A análise SWOT da Operação Absolute Resolve identifica como forças a sincronia multidomínio entre inteligência, comandos cibernéticos e forças especiais que criou "corredores cibernéticos" para neutralizar defesas, e a precisão cirúrgica que permitiu captura de alvos sem baixas através de geointeligência satelital e dispositivos de localização.

Figura 1: Análise SWOT da Operação Absolute Resolve.

As fraquezas incluem a dependência de nó tecnológico único (satélite ou *link* cibernético) cuja falha comprometeria a operação, e a complexidade de planejamento que exige meses de preparação, limitando resposta a crises imediatas.

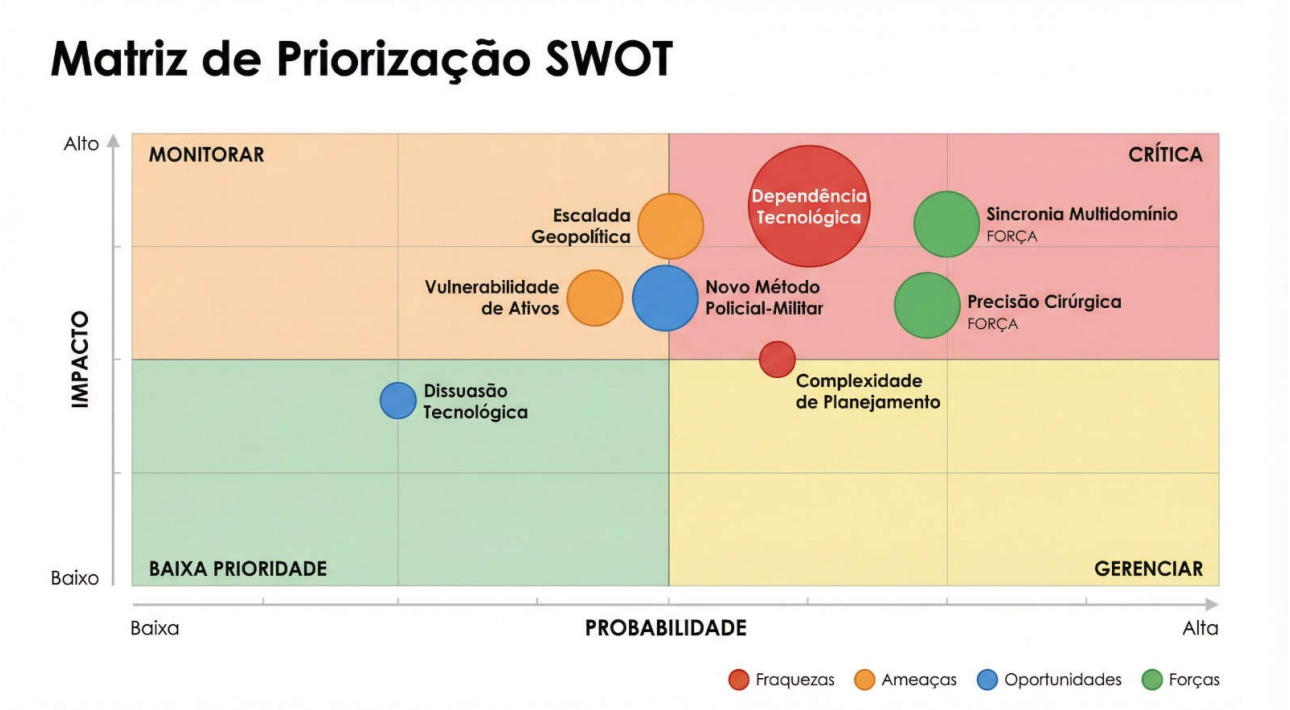

Figura 2: Matriz de Priorização SWOT da Operação Absolute Resolve.

Externamente, as ameaças abrangem a escalada geopolítica com adversários desenvolvendo contramedidas cibernéticas assimétricas e capacidades antissatélite, além da vulnerabilidade de ativos sensíveis em território hostil com risco de engenharia reversa.

Já as oportunidades externas residem no novo método policial-militar como instrumento de projeção de poder e na dissuasão tecnológica mostrando que fortificações modernas podem ser contornadas sem destruição física. A prioridade é mitigar a dependência tecnológica através de redundância em sistemas satelitais e cibernéticos enquanto se capitaliza oportunidades metodológicas e se protegem ativos sensíveis contra comprometimento.

DISCUSSÃO: A DOUTRINA DE OPERAÇÕES CIBERNÉTICAS

Um ponto que podemos discutir e cada leitor pode com base em sua experiência debater em grupo, é a aplicação prática da C-SEAD. Ao invés de bombas cinéticas, utilizou-se a alteração de localização de alvos e a interrupção da cadeia de comando. Ao explorar o tempo de reação do inimigo e sua pronta resposta, as forças americanas garantiram princípios da guerra: surpresa, velocidade e concentração de massa no ponto decisivo, bem como fatores de combate: movimento/manobra, segurança, inteligência e fogos.

Isto para nossas Forças Armadas é decisivo para uma urgente revisão dos protocolos de contrainteligência e inserção nos Jogos de Guerra do Ministério da Defesa e do Estado-Maior Conjunto quanto às infraestruturas críticas e estratégicas nacionais.

LIÇÕES PRIMORDIAIS PARA O BRASIL

De mais a mais, a operação americana de assalto para captura, embora um estudo de caso hipotético de um adversário regional, oferece lições estratégicas inadiáveis para o Brasil e nossas Forças Armadas, especialmente no contexto da defesa de infraestruturas críticas dos poderes Político, Energético e Econômico. São elas:

Soberania e Resiliência nos Domínios Cibernético e Espacial: A lição primordial é que a defesa nacional moderna é decidida no ciberespaço e no espaço. O Brasil deve acelerar o investimento no desenvolvimento de capacidades de Guerra Cibernética e Eletrônica (G Ciber/GE) ofensivas e defensivas, garantindo a resiliência de nossos ativos espaciais (satélites de comunicação e sensoriamento remoto) e infraestruturas críticas, sempre com redundância, dispersão e proteção contra mísseis (ativos da Força Aérea e

da Marinha do Brasil). A capacidade de “cegar” ou desabilitar o inimigo ou proteger seus próprios sistemas é o novo pré-requisito para qualquer manobra militar.

Integração Doutrinária Multidomínio (MDO): As Forças Armadas Brasileiras devem transcender a simples coordenação interforças e buscar a integração doutrinária total. O planejamento de qualquer operação, seja terrestre, naval ou aérea, deve começar com a negação cibernética e eletrônica do inimigo, garantindo que a superioridade informacional seja estabelecida antes da manobra física.

Inteligência de Precisão e GEOINT: Pode-se concluir sem margem para erros que a tecnologia é inútil sem a inteligência de campo (HUMINT) de alta precisão e a capacidade de transformá-la em Geointeligência (GEOINT) acionável. Destarte, o Brasil deve investir paralelamente aos projetos estratégicos em andamento na integração de dados de satélites e drones com as forças operacionais, permitindo o mapeamento de “padrões de vida” e a localização de alvos em ambientes complexos, como a selva amazônica ou áreas urbanas densas.

FORÇAS ESPECIAIS COMO VETOR DE PROJEÇÃO TECNOLÓGICA

Outro ponto nevrálgico é que as forças especiais brasileiras (Comandos e Forças Especiais) devem ser empregadas como o principal vetor para a aplicação de poder em cenários de guerra irregular e de alto risco. Elas devem ser o foco da integração tecnológica multidomínio, utilizando a discrição e a precisão para aplicar o poder cibernético e eletrônico no ponto de impacto tático, como se tem visto nas guerras modernas pela Rússia e Israel.

À GUISA DE CONCLUSÃO

Isto posto, temos que a Operação Absolute Resolve serve como o “padrão-ouro” para as operações especiais da década de 2030. Digna de nota é a integração da guerra eletrônica, cibernética e espacial não mais como suporte, mas como espinha dorsal da manobra militar.

A capacidade de “cegar” o inimigo e capturar alvos em seus redutos mais protegidos demonstra que a geografia e a fortificação física são secundárias à superioridade no domínio da informação.

Para o futuro, o desafio reside na manutenção dessa vantagem tecnológica frente a

adversários que buscam a paridade cibernética. Temos aí uma lição para o Brasil: mesmo com diversos projetos estratégicos em andamento, é necessário buscar verbas "secretas" para projetos também "secretos" que busquem sobrepujar eventuais potências nucleares.

Para nós brasileiros, independe do governo o êxito em uma operação militar: nos cabe identificar oportunidades e ameaças e buscar a defesa da soberania do país independentemente do Poder Público, seja no campo acadêmico, nas audiências públicas, seja recorrendo à participação popular nos assuntos de defesa, como disposto na Política Nacional de Defesa.

REFERÊNCIAS

WALTERS, Ryan. *Information Warfare: The Army's Continuous Transformation in Action*. Small Wars Journal, 15 de janeiro de 2026. Disponível em: https://smallwarsjournal.com/2026/01/15/army-information-warfare-transformation

WRIGHT, Rebecca. *Multi-domain Dominance*. U.S. Army, 14 de agosto de 2024. Disponível em: https://www.army.mil/article/279765/multidomain_dominance

PRIEBE, Miranda; **LIGOR**, Douglas C.; **MCCLINTOCK**, Bruce; **SPIRTAS**, Michael; **SCHWINDT**, Karen; **LEE**, Caitlin; **RHOADES**, Ashley L.; **EATON**, Derek; **HODGSON**, Quentin E.; **ROONEY**, Bryan. *Multiple Dilemmas: Challenges and Options for All-Domain Command and Control*. Rand Corporation, 2020. Disponível em: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA300/RRA381-1/RAND_RRA381-1.pdf

LUND-HANSEN, Katrine e **REILLY**, Jeff. *The Multi-Domain Operations Approach to Intermediate PME*. Army War College; War Room Online Journal, 1º de novembro de 2024. Disponível em: https://warroom.armywarcollege.edu/articles/competencies-6

NGA. *Geospatial Intelligence (GEOINT) Basic Doctrine*. National System for Geospatial Intelligence, abril de 2018. Disponível em: https://www.nga.mil/assets/files/170901-038_GEOINT_Basic_Doctrine_Pub_1.pdf

***Carlos A. Klomfahs** é advogado, especialista em Direito Internacional dos Conflitos Armados e operador de Inteligência. Egresso curso de geopolítica da ECEME e estratégia marítima da Escola de Guerra Naval. É mestrando no Programa de Pós-Graduação em Segurança Internacional e Defesa (PPGSID) da Escola Superior de Guerra.*