Integrantes da Companhia A, 1º Batalhão, 111º Regimento de Infantaria, 56ª Brigada de Combate *Stryker*, conduzem uma iteração noturna de tiro real de um adestramento de armas combinadas durante o Exercício *Decisive Strike* 2019 no Centro de Apoio ao Treinamento em Krivolak, na Macedônia do Norte, 11 de junho de 2019. (Foto: 2º Sgt Frances Ariele L. Tejada, Exército dos EUA)

Utilização da Dissimulação Militar em Múltiplos Domínios para Expor o Inimigo em 2035

Ten Cel Stephan Pikner, Ph.D., Exército dos EUA

O problema operacional que o Exército enfrentará no ano de 2035 será fundamentalmente diferente dos que ele enfrentou anteriormente. O antigo desafio, para o qual as atuais plataformas e doutrina do Exército dos Estados Unidos da América (EUA) ainda estão otimizadas, era um problema solucionado por meio da ruptura do segundo escalão de forças de assalto soviéticas com fogos de precisão de longo alcance, interdição aérea de asa fixa e ataques profundos por aeronaves de ataque de asa rotativa. Hoje, e mais ainda em 2035, as grandes potências rivais emergentes dos EUA representam um desafio completamente diferente. Ao ameaçar o acesso dos EUA a um teatro de operações e negar as zonas de reunião necessárias à concentração para um contra-ataque decisivo, seus adversários minaram o modo de guerra expedicionário, preferido pelo país. Essa abordagem de antiacesso/negação de área (*anti-access/area denial*, A2/AD) bloqueia a capacidade de responder eficazmente a uma agressão rápida e limitada, o que deixa aliados e parceiros vulneráveis a uma ampla gama de atividades coercitivas e subversivas.[1] Algo central ao A2/AD é uma rede bem defendida, redundante e, em grande parte, oculta de sensores e sistemas de armas que possam localizar, visar e atacar forças amigas que estejam entrando e se concentrando em um teatro de operações.[2] Para enfrentar esse desafio, o Exército deve adotar uma nova abordagem para localizar e fixar os componentes críticos do complexo de A2/AD de um adversário, a fim de garantir a liberdade de ação em 2035.

Para localizar os principais nós da rede de A2/AD de um adversário em 2035, será preciso inverter a lógica tradicional de reconhecimento. Embora regimentos de cavalaria possam buscar, eficazmente, informações sobre a disposição dos escalões inimigos em avanço, localizar os componentes críticos de um complexo integrado de A2/AD é uma questão completamente diferente. Em vez de exporem forças amigas vulneráveis conforme elas buscarem, metodicamente, um adversário geralmente estático e bem camuflado com fogo e manobra, as futuras forças terrestres podem induzir um oponente a desmascarar os sensores e meios de ataque de longo alcance centrais ao seu sistema de A2/AD mediante o uso da dissimulação militar em múltiplos domínios. Em particular, essa forma de estimular o complexo de busca de alvos e ataque de um adversário deve levar em consideração como serão tomadas decisões apoiadas na inteligência artificial (IA). No futuro próximo, os adversários dos EUA provavelmente utilizarão esses sistemas automatizados para combinar uma ampla gama de informações em propostas de alvos a serem submetidas à tomada de decisões humana. Ao desencadear o acionamento e emprego prematuros de meios de alto valor de um adversário em sua tentativa de localizar, fixar e atacar alvos falsos ou fantasmas estadunidenses, a dissimulação militar em múltiplos domínios pode ser central para um esforço integrado de localizar e destruir o inimigo nos campos de batalha futuros.

Este argumento de que a dissimulação militar em múltiplos domínios é central para a localização de adversários dos EUA nos campos de batalha de 2035 é organizado em três partes. Primeiro, são apresentados, de forma breve, os antecedentes doutrinários da dissimulação militar em sua forma atual. Segundo, e de forma mais detalhada, apresenta-se uma análise sobre a provável evolução dos sistemas de A2/AD adversários, com foco nos pontos fortes e potenciais fraquezas do apoio de IA à busca de alvos. Terceiro, apresenta-se uma série de recomendações que o Exército deve considerar a fim de empregar, da melhor forma, a dissimulação em múltiplos domínios para localizar o inimigo em 2035, com exércitos de campanha centrados em grandes potências como o integrador dessas atividades.

Um robô TALON controlado por um técnico de desativação de artefatos explosivos (*explosive ordnance disposal*, EOD), designado para a Unidade EOD Móvel 2, aproxima-se de um item suspeito durante o adestramento noturno sobre artefatos explosivos improvisados realizado na Base Conjunta Expedicionária Little Creek-Fort Story, Virginia Beach, na Virgínia, 17 de abril de 2019. (Foto: MCC Jeff Atherton, Marinha dos EUA)

Antecedentes doutrinários da dissimulação militar

Os antecedentes doutrinários e históricos da dissimulação militar já são bem estabelecidos. Em linhas gerais, as atividades de dissimulação militar "são planejadas e executadas para fazer com que os adversários tomem ações ou inações que sejam favoráveis aos objetivos do comandante".[3] No contexto específico de estimular um sistema de A2/AD adversário, isso envolve amplificar assinaturas de unidades de despistamento e substituir, continuamente, as assinaturas de unidades reais pelas de unidades simuladas, sobrecarregando, assim, um adversário com um número enorme de falsos positivos.[4] Essa abordagem de gerar um grande número de falsos positivos — a impressão de existirem alvos quando, na verdade, não há nenhum — contrasta com a noção tradicional de camuflagem, que tenta criar um falso negativo, de não haver nenhum alvo, mascarando as assinaturas de forças amigas. Algo central para o êxito dos esforços de dissimulação é seu caráter de múltiplos domínios. Em uma era de sensores cada vez mais difundidos, sofisticados e variados, enganar apenas um tipo deles pouco faz contra um adversário capaz de combinar rapidamente diversas fontes de informação. A "dissimulação em múltiplos domínios", conforme propôs Christopher Rein, "requer uma coordenação estreita e minuciosa em todos os domínios de combate, para garantir que lapsos em um deles não anulem esforços em outras áreas".[5]

A provável evolução dos sistemas de A2/AD adversários

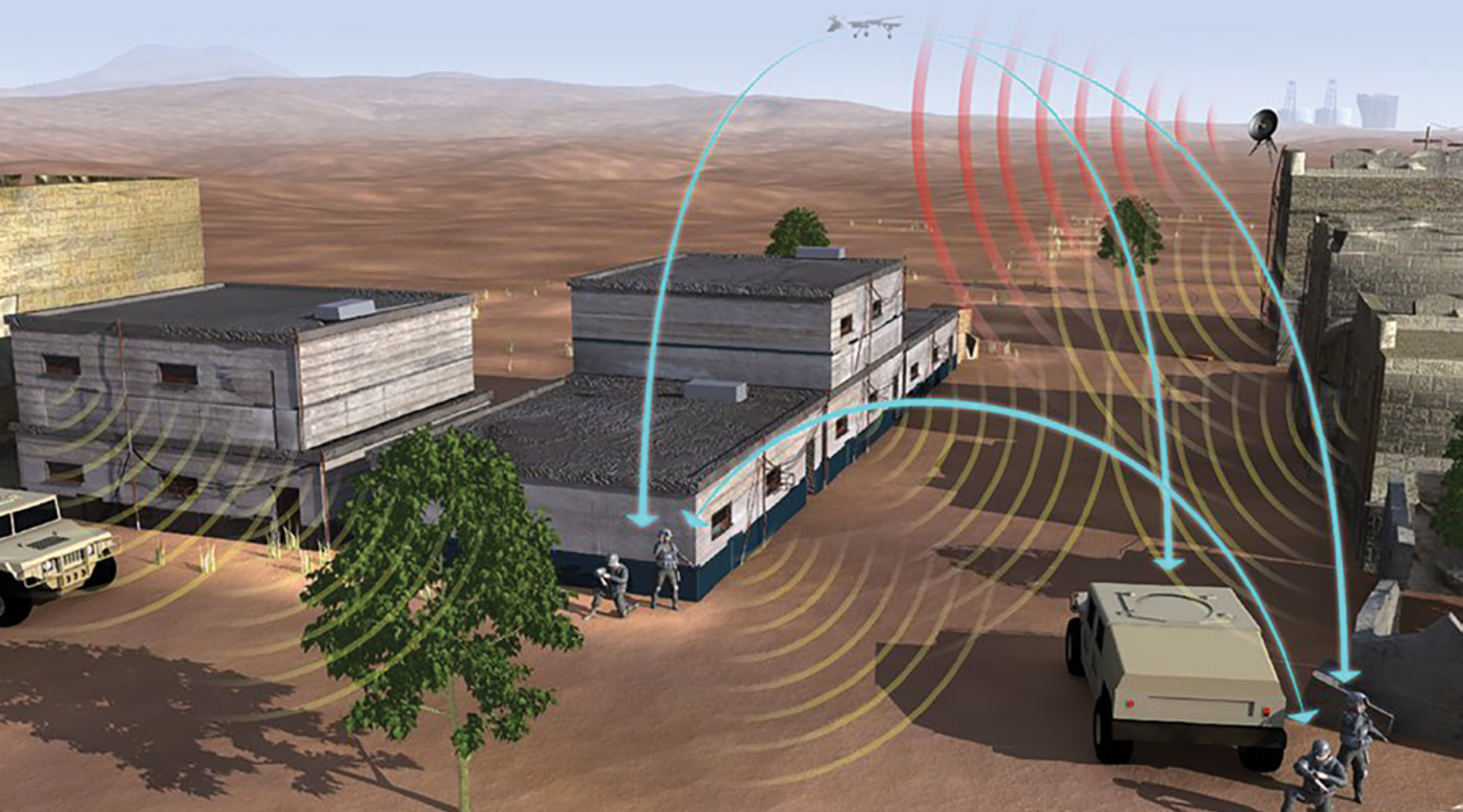
Obter um entendimento correto da arquitetura de A2/AD de um oponente requer a integração de informações colhidas por uma variedade de meios. A dependência excessiva de um único método, como a interceptação de comunicações eletrônicas ou as imagens aéreas, pode resultar em lacunas intransponíveis no entendimento. Os EUA são, há muito, incomparáveis em sua consciência do campo de batalha, mas as grandes potências rivais vêm ganhando terreno rapidamente devido a dois fatos inter-relacionados. Em primeiro lugar, a maior sofisticação, fidelidade, custo acessível e variedade de sensores tornaram a coleta de informações militarmente relevantes mais fácil e econômica. Contudo, transformar essas informações em entendimento requer um segundo passo, e sua automatização iminente pode mostrar-se revolucionária.

A promessa do aprendizado de máquina de combinar e converter informações brutas, de forma rápida e precisa, em propostas de alvos dificultará bastante as tarefas de ocultar — e sobreviver — no futuro campo de batalha.

Avanços difundidos em plataformas e sensores comerciais de baixo custo, como drones e câmeras de alta resolução, juntamente com informações de fontes abertas quase em tempo real, como postagens nas mídias sociais e imagens de satélite disponíveis comercialmente, transformaram tanto a escala quanto a fidedignidade das informações disponíveis e o número de atores internacionais com acesso a elas. Antes disponíveis apenas para as principais potências, esses sensores proliferaram amplamente nas últimas décadas. Essa tendência não mostra sinais de redução. À medida que os meios de detecção se tornarem mais baratos, confiáveis e capazes de colher informações de alta qualidade, a vantagem informacional com a qual os EUA contaram nas últimas décadas diminuirá ainda mais.[6]

Aumentar a diversidade e a qualidade dos meios de coleta de informações resolve metade do desafio. A segunda metade — combinar informações de várias fontes para criar um quadro detalhado de um alvo — é uma tarefa mais difícil. Atualmente, esse é um processo trabalhoso, o qual envolve equipes multifuncionais de analistas que examinam, minuciosamente, uma enorme quantidade de dados captados por sensores com uma resolução cada vez maior. Segundo uma estimativa, seria preciso "oito milhões de pessoas só para analisar todas as imagens do mundo que serão geradas nos próximos 20 anos".[7] No entanto, avanços no aprendizado de máquina podem melhorar e acelerar significativamente a fusão das informações colhidas. Os classificadores baseados em aprendizado de máquina, que "tomam uma amostra de entrada e a identificam como uma de várias classes de saída", são particularmente adequados à fusão de informações e busca de alvos.[8] Em um contexto de apoio de IA à busca de alvos de A2/AD, a amostra de entrada consistiria nos dados colhidos por uma gama de sensores, e as classes de saída seriam uma classificação do alvo. Um algoritmo de aprendizado de máquina devidamente treinado e com acesso a uma ampla gama de dados corretos

Novas tecnologias converterão e integrarão sinais eletromagnéticos de várias fontes em dados digitais que possam ser processados a velocidades inéditas, de modo a melhorar a capacidade do combatente para perceber medidas de dissimulação inimigas, a fim de identificar e neutralizar ameaças no campo de batalha moderno. Os avanços tecnológicos também aumentarão drasticamente a capacidade de forças amigas para iludir esforços inimigos de coleta de inteligência por meio de medidas melhores de guerra eletrônica. (Ilustração: cedida por Defense Advanced Research Projects Agency)



seria, então, capaz de encontrar a proverbial "agulha no palheiro" e classificar devidamente um alvo, acelerando e melhorando, em grande medida, o processo de fusão de informações, que era, até então, algo trabalhoso.[9]

À semelhança de sua decrescente vantagem em relação a sensores, os EUA não deterão o monopólio sobre essas técnicas de fusão automatizadas. Até 2035, os adversários dos EUA provavelmente terão explorado técnicas de aprendizado de máquina para combinar informações colhidas de uma ampla gama de sensores para visar suas armas de A2/AD. Isso apresentará uma nova série de desafios para o modo como as forças amigas se ocultam. A coleta substancial de uma ampla gama de assinaturas de forças amigas pode anular seus esforços para camuflar de uma forma unidimensional. Por exemplo, minimizar emissões eletromagnéticas pode ter um efeito insignificante contra um adversário que ainda possa detectar a assinatura térmica, de empresas contratadas civis ou de mídias sociais de uma unidade. Em termos mais gerais, será quase impossível criar um falso negativo coeso contra um sistema de sensores extremamente sensíveis em múltiplos domínios — o adversário detectará algo e uma IA bem treinada será capaz de extrapolar e gerar um quadro correto do alvo a partir do que houver sido detectado.

Embora desafiadora, essa potencial revolução nas técnicas de coleta e fusão de informações de um adversário dos EUA representa uma oportunidade para que as forças amigas localizem o inimigo nos campos de batalha de 2035. Se feita de forma coesa, a nova dissimulação militar em múltiplos domínios pode distorcer os algoritmos de um adversário e explorar as tensões organizacionais e de procedimento entre propostas produzidas por aprendizado de máquina e os decisores humanos. Essa dissimulação não é um fim em si mesmo. Para esclarecer as informações duvidosas e contraditórias para decisões sobre alvos, um adversário será forçado a expor sua arquitetura de A2/AD ao usar meios cada vez mais ativos, que emitem assinaturas inequívocas. Iludir um adversário, levando-o a expor os nós cruciais de sua arquitetura de A2/AD é fundamental para localizar forças inimigas bem escondidas em 2035.

O aprendizado de máquina não é impermeável à falsificação ou dissimulação de dados. O aprendizado de máquina se apoia mais em dados prontamente quantificáveis como entradas do que os processos existentes, nos quais seres humanos podem colocar evidências ambíguas em contexto. Sensores concentrados estritamente em detectar dados específicos e mensuráveis eletromagnéticos, acústicos, térmicos, gravitacionais, visuais, vibracionais, georreferenciados de mídias sociais ou de análise de texto assistida por computador devem ser alimentados de forma limpa em um algoritmo de aprendizado de máquina. Esse algoritmo, por sua vez, é treinado por meio da formação de correlações entre assinaturas semelhantes e características conhecidas do alvo.[10] Sua exatidão depende da riqueza de seu conjunto de dados de treinamento, onde verdadeiros positivos e covariáveis válidas e associadas formam uma base para o algoritmo ser ajustado e atualizado. Em um contexto militar, os verdadeiros positivos seriam casos reais do alvo e as covariáveis associadas seriam a gama completa de assinaturas mensuráveis em todos os domínios. Atualmente, a fusão de informações de múltiplos domínios acontece por meio de células com grande necessidade de pessoal nos estados-maiores. O aprendizado de máquina oferece a oportunidade para que esse mesmo processo ocorra rapidamente, automaticamente e por meio do reconhecimento de padrões de correlações que podem passar despercebidos à cognição humana. Gerar confusão deliberadamente por meio de operações de dissimulação militar que obscureçam a aparência de um verdadeiro alvo pode minar esse processo de aprendizado, levando um sistema de A2/AD apoiado em IA a buscar as assinaturas erradas no lugar errado. Ou, conforme expressaram Edward Geist e Marjory Blumenthal, as forças amigas podem empregar "máquinas de névoa da guerra" para confundir sensores adversários e os processos associados de aprendizado de máquina.[11]

O Ten Cel Stephan Pikner, Ph.D., do Exército dos EUA, é estrategista do Exército (Área Funcional 59), formado pelo Advanced Strategic Policy and Planning Program. Concluiu o bacharelado pela Academia Militar dos EUA, mestrado em Administração Pública pela Harvard Kennedy School of Government e doutorado pela Georgetown University. Serviu, mais recentemente, como Subchefe de Planejamento (G5) do Comando Aliado Terrestre da Organização do Tratado do Atlântico Norte (OTAN) em Izmir, na Turquia.

Essa maior dependência em relação a fluxos de dados quantificáveis para alimentar um algoritmo de busca de alvos baseado no aprendizado de máquina também pode gerar uma vulnerabilidade crítica dentro da organização de um adversário: ela vem à custa da experiência e intuição humana, tornando todo o sistema vulnerável à dissimulação em múltiplos domínios. O desenvolvimento intermitente e desigual da IA ao longo das últimas décadas está repleto de exemplos de máquinas aparentemente inteligentes que, quando confrontadas com desafios da vida real fora do alcance restrito de seu treinamento, ficaram completamente desnorteadas.[12] Ao contrário dos sistemas programados de modo convencional, não há uma equipe de engenheiros que possam ajustar facilmente o código para apoiar melhor os decisores humanos no sistema, e sim uma caixa preta, em que as saídas são geradas por camadas ocultas de conexões ponderadas dentro de uma rede neural formada pela iteração dos dados de treinamento.[13] Essa falta de clareza sobre como a máquina aprende pode gerar fricção em um sistema de tomada de decisão humana apoiado por IA. Antes de uma falha no mundo real, a pressuposta onisciência de um algoritmo de aprendizado de máquina pode diminuir o valor relativo do processo decisório humano. Isso cria um dilema: quando o sistema de aprendizado de máquina é mais necessário, menos se confia nele, enquanto a alternativa baseada na decisão humana se atrofiou em status e capacidade.[14]

Enganar o sistema de busca de alvos baseado em aprendizado de máquina de um adversário pode levá-lo a ativar sensores com forte assinatura ou a atacar alvos falsos. Em futuros conflitos terrestres, isso cria uma importante janela de oportunidade para produzir fogos de contrabateria conjuntos de forças amigas contra a "cadeia de ataque" (*kill chain*[NT1]) de sensores, nós de comando e controle e plataformas de armas do inimigo.[15] O que a dissimulação militar em múltiplos domínios traz para o futuro combate é o potencial de enganar a máquina — de confundir uma cadeia de busca de alvos de um adversário apoiada por IA — e, por meio de tal dissimulação, expor seus meios de reconhecimento e ataque.

NT1: O conceito de "kill chain" está ligado ao de "dynamic targeting", ou "alvejamento dinâmico" (localizar, fixar, alvejar, rastrear, engajar e avaliar). Veja JP 3-09, *Joint Fire Support*, p. xii, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_09.pdf.

Recomendações

Desenvolver e implementar as organizações, doutrina, treinamento e equipamentos necessários para o emprego eficaz da dissimulação militar em múltiplos domínios requer uma abordagem deliberada e coordenada.[16] Esta seção descreve quatro considerações específicas para uma força capaz de utilizar a dissimulação em múltiplos domínios para localizar o inimigo em 2035. Primeiro, os componentes de um dispositivo integrado de dissimulação em múltiplos domínios devem ser flexíveis e adaptáveis, para manter um efeito contínuo contra um adversário que aprende. Segundo, a dissimulação em múltiplos domínios no amplo espectro não pode começar em uma crise, mas fundamentar-se em condições de referência, definidas durante a competição abaixo do limiar do conflito armado. Terceiro, como é extremamente provável que as operações terrestres envolvam aliados e parceiros que combaterão ao lado das forças terrestres estadunidenses, a dissimulação em múltiplos domínios será reforçada pela inclusão deles em um plano que englobe todo o teatro de operações. Por último, a dissimulação em múltiplos domínios não deve ser vista como um fim em si mesmo, mas como um meio de levar um adversário a "mostrar as cartas". Ao provocar a cadeia de ataque de A2/AD de um inimigo, levando-o a perseguir formações fantasmas, a dissimulação em múltiplos domínios pode estimular — e, portanto, expor — componentes críticos de sua rede à destruição.

A primeira consideração no desenvolvimento da dissimulação em múltiplos domínios é a dinâmica interativa, competitiva e evolutiva da dissimulação militar. O êxito da dissimulação depende tanto das percepções e interpretações de um adversário em relação às assinaturas de forças amigas quanto das emissões geradas pelas formações. Além das dimensões técnicas da geração de aparições convincentes, há um elemento organizacional crucial baseado na cultura militar do adversário dos EUA: o que pode enganar estadunidenses pode não iludir um adversário, e métodos que podem ser eficazes contra um rival podem ser descartados por outro. Os esforços de dissimulação devem adaptar-se continuamente conforme os vieses, capacidades e doutrina do adversário evoluírem.

Segundo, uma dissimulação bem-sucedida durante a crise de um conflito deve ser desenvolvida sobre uma base estabelecida em tempo de paz. A

competição persistente abaixo do limiar do conflito armado deve incluir esforços deliberados para monitorar, mascarar e simular o amplo espectro de assinaturas de forças terrestres amigas. Isso tem dois objetivos: primeiro, "ver a nós mesmos" de modo abrangente; e, segundo, influenciar os conjuntos de dados de treinamento que os adversários dos EUA vêm desenvolvendo com respeito às forças amigas em tempo de paz para treinar seus sistemas de busca de alvos baseados em IA. Para alcançar esses objetivos, as operações de tropas amigas em tempo de paz devem ser monitoradas de forma detalhada por equipes encarregadas de desenvolver um perfil abrangente das assinaturas e emissões de uma unidade. Esse perfil será a referência do que pode ser detectado e explorado pelos sensores de A2/AD de um adversário. Essas equipes monitorariam forças amigas em simulações de engajamentos táticos e durante desdobramentos reais em áreas de operações. A partir desses dados, colhidos na competição em tempo de paz durante rodízios de desdobramento e exercícios, pode-se criar um quadro completo e no amplo espectro de como as formações terrestres aparecem para a gama completa de sensores de um adversário.

Essa assinatura abrangente de forças amigas catalogada em tempo de paz pode ser utilizada de duas maneiras. A primeira é mascarar a presença de forças verdadeiras, minimizando suas emissões. Ao contrário da crença geral de "treinar como se combate", muitas das medidas que seriam utilizadas para mascarar a presença de uma unidade só devem ser tomadas em uma crise no mundo real. Praticá-las rotineiramente durante a competição em tempo de paz permitiria que um adversário aprendesse sinais alternativos da localização e disposição de uma unidade que são mais difíceis (ou impossíveis) de mascarar durante um conflito. Por exemplo, minimizar a assinatura eletromagnética de uma unidade durante um rodízio de desdobramento pode levar um adversário a procurar mais minuciosamente outras assinaturas, que não sejam tão fáceis de ocultar, como principais indicadores das forças amigas.

Além de servir de base para a melhor forma de mascarar a verdadeira localização de uma unidade amiga em crise, a assinatura abrangente de forças amigas pode ser reproduzida como uma técnica de dissimulação. Essa assinatura inclui não apenas os equipamentos militares de uma força amiga, mas também as emissões das mídias sociais e de empresas contratadas comerciais que são produzidas pelo desdobramento de tal força. Unidades de dissimulação amigas que possam simular as características de formações de combate completas podem atuar como "potes de mel", que desviem a atenção para longe das forças reais e levem o inimigo a expor componentes cruciais de sua cadeia de ataque de A2/AD.

Terceiro, é quase certo que o futuro combate no domínio terrestre ocorrerá em um contexto de coalizão. Para maximizar a eficácia tática da dissimulação militar em múltiplos domínios, as assinaturas de forças terrestres aliadas e parceiras devem ser medidas e reproduzidas de uma forma semelhante às de forças terrestres estadunidenses. No nível do teatro de operações, isso inclui operações de dissimulação militar envolvendo portos de desembarque, centros de forças estratégicas e outras infraestruturas críticas que capacitem a escalada de forças amigas em uma área de operações. Como essas instalações estão, com frequência, localizadas perto de centros populacionais e têm, normalmente, funções tanto civis quanto militares, deve ser dada especial consideração às preocupações de aliados e restrições sobre atividades de dissimulação militar. Linhas claras reforçando o status de proteção de certas instalações e pessoal (por exemplo, hospitais, locais religiosos, pessoal médico) devem ser elaboradas e comunicadas aos aliados dos EUA para evitar qualquer percepção de que esses esforços violariam o Direito Internacional dos Conflitos Armados.[17]

Por fim, o objetivo geral desse esforço de dissimulação militar em múltiplos domínios é localizar o inimigo nos campos de batalha do futuro. É ao apresentar um alvo irresistível, mas falso, ao adversário que a dissimulação militar em múltiplos domínios facilita a localização do inimigo. Estimular o sistema integrado de sensores e armas de um inimigo com a simulação da presença de alvos vantajosos, mas falsos, pode expor os meios de alto valor e com alta capacidade de sobrevivência de sua cadeia de ataque. A dissimulação eficaz pode acionar uma gama completa de sensores adversários — equipes de reconhecimento, sistemas de ataque eletrônico, satélites, veículos aéreos não tripulados, radares de vigilância terrestre e meios cibernéticos — levando à sua ativação em busca de uma quimera. As armas de A2/AD de um inimigo, como mísseis balísticos no teatro de

operações, artilharia de longo alcance e forças especiais, também seriam empregadas a partir de locais seguros e camuflados para atacar o que eles acreditariam serem concentrações reais de forças amigas. Prevendo essa ativação, os sistemas de inteligência, vigilância e reconhecimento de forças amigas, sincronizados com o plano de dissimulação militar em múltiplos domínios, poderiam antever, detectar e explorar essa atividade aberta e ativa do inimigo. Em vez de uma busca ineficaz e dispendiosa contra componentes fortalecidos e camuflados de um sistema de A2/AD, a dissimulação militar em múltiplos domínios pode enganar nossos futuros adversários e levá-los a expor-se prematuramente.

A implementação dessas recomendações requer o entendimento detalhado de uma grande potência rival, o nível adequado de autorizações e capacidades de forças amigas e o dispositivo de forças durante a competição abaixo do limiar do conflito armado para manter e modular uma campanha de dissimulação prolongada. Na estrutura atual do Exército dos EUA, essa tarefa provavelmente se encaixaria entre o corpo de exército e o comando componente[NT2] relevante do Exército. Conforme o Exército se adaptar à competição entre grandes potências, a recomendação final deste artigo é que um exército de campanha, centrado em competir contra um adversário específico, seja o responsável e integrador das operações de dissimulação militar em múltiplos domínios.[18] Sem o peso das responsabilidades do comando componente do Exército no âmbito de todo o teatro de operações e diferentemente de um corpo de exército dirigido contra um adversário específico na competição em tempo de paz, um exército de campanha estaria mais bem posicionado para conceber e executar uma campanha de dissimulação militar prolongada, coesa e especialmente adaptada. Por meio dessa dissimulação, o Exército dos EUA poderá forçar seus adversários a atacar sombras cegamente, expondo os componentes cruciais de sua arquitetura de A2/AD à detecção, destruição e, por fim, derrota. ■

NT2: Os comandos componentes do Exército dos EUA são: USARAF, USARCENT, USARNORTH, USARSOUTH, USAREUR, USARPAC, USASOC, SDDC, USASMDC e ARCYBER. Veja "Organization: Understanding the Army Structure", https://www.army.mil/organization/.

Referências

1. Andrew J. Duncan, "New 'Hybrid War' or Old 'Dirty Tricks'? The Gerasimov Debate and Russia's Response to the Contemporary Operating Environment", *Canadian Military Journal* 17, no. 3 (Summer 2017): p. 6-11.

2. Wilson C. Blythe Jr. et al., *Unclassified Summary of the U.S. Army Training and Doctrine Command Russian New Generation Warfare Study* (Fort Leavenworth, KS: Army University Press, 2020), acesso em 20 out. 2020, https://www.armyupress.army.mil/Portals/7/online-publications/documents/RNGW-Unclassified-Summary-Report.pdf?ver=2020-03-25-122734-383.

3. Field Manual 3-13.4, *Army Support to Military Deception* (Washington, DC: U.S. Government Publishing Office, 2019), 1-2.

4. Ibid., 1-8.

5. Christopher M. Rein, ed., "Multi-Domain Deception", in *Weaving the Tangled Web: Military Deception in Large-Scale Combat Operations* (Fort Leavenworth, KS: Army University Press: 2018), p. 2.

6. Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton, NJ: Princeton University Press, 2010).

7. Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare* (New York: Hatchette, 2020), p. 59.

8. Patrick McDaniel, Nicolas Papernot, and Z. Berkay Celik, "Machine Learning in Adversarial Settings", *IEEE Security & Privacy* 14, no. 3 (May 2016): p. 68-72.

9. Stephan Pikner, "Training the Machines: Incorporating AI into Land Combat Systems", Landpower Essay Series (Washington, DC: Institute of Land Warfare, January 2019), acesso em 20 out. 2020, https://www.ausa.org/sites/default/files/publications/LPE-19-1-Training-the-Machines-Incorporating-AI-into-Land-Combat-Systems.pdf.

10. Gary Marcus, "Deep Learning, a Critical Appraisal" (artigo, New York University, 2018), acesso em 20 out. 2020, https://arxiv.org/ftp/arxiv/papers/1801/1801.00631.pdf.

11. Edward Geist and Marjory Blumenthal, "Military Deception: AI's Killer App?", War on the Rocks, 23 October 2019, acesso em 20 out. 2020, https://warontherocks.com/2019/10/military-deception-ais-killer-app/.

12. Marcus, "Deep Learning, a Critical Appraisal".

13. McDaniel, Papernot, and Celik, "Machine Learning in Adversarial Settings".

14. Peter Hickman, "The Future of Warfare Will Continue to Be Human", War on the Rocks, 12 May 2020, acesso em 20 out. 2020, https://warontherocks.com/2020/05/the-future-of-warfare-will-continue-to-be-human/.

15. Brose, *The Kill Chain*.

16. Eric Wesley and Jon Bates, "To Change an Army—Winning Tomorrow", *Military Review* 100, no. 3 (May-June 2020): p. 6-18. [NT: O artigo traduzido, intitulado "Para Mudar um

Exército: Vencendo Amanhã", consta da edição brasileira do Quarto Trimestre de 2020, https://www.armyupress.army.mil/Journals/Edicao-Brasileira/Arquivos/Quarto-Trimestre-2020/Para-Mudar-um-Exercito-Vencendo-Amanha/.]

17. "Geneva Convention (IV): Relative to the Protection of Civilian Persons, Part I", Infoplease, 12 August 1949, acesso em 2 nov. 2020, https://www.infoplease.com/primary-sources/government/united-nations/convention-relative-protection-civilian-persons-time-war.

18. Amos C. Fox, "Getting Multi-Domain Operations Right: Two Critical Flaws in the U.S. Army's Multi-Domain Operations Concept", Land Warfare Paper 133 (Washington, DC: Association of the United States Army, June 2020), acesso em 20 out. 2020, https://www.ausa.org/sites/default/files/publications/LWP-133-Getting-Multi-Domain-Operations-Right-Two-Critical-Flaws-in-the-US-Armys-Multi-Domain-Operations-Concept.pdf.