

Onde se Esconder

O Aumento de Ameaças às Bases Aéreas

Cel Shannon W. Caudill, *USAF*
Maj Benjamin R. Jacobson, *USAF*

Os agressores em uniformes do Exército norteamericano penetraram as defesas da base aérea de noite. Armados com rifles, obuses e coletes suicidas, a equipe de 14 homens iniciou sua missão letal contra a base aérea na Província de Helmand, Afeganistão, guarnecida pela Força de Assistência à Segurança Internacional [*International Security Assistance Force - ISAF*] da OTAN. Seguiram-se horas de combate. A alvorada revelou a destruição de seis jatos *AV-8B Harrier* e dano a outras duas aeronaves. Além do mais “seis hangares foram danificados” e “seis postos de reabastecimento de combustível destruídos”.¹ O ataque resultou em morte de catorze insurgentes e de dois Fuzileiros Navais. Oito membros da coalizão e um empreiteiro foram feridos. Até a presente data, essa operação insurgente em setembro de 2012 foi o ataque terrestre mais bem sucedido contra as tropas e equipamento da *ISAF* no conflito afegão.

O famoso General italiano Giulio Douhet notou que “é mais fácil e eficaz arrasar o poder aéreo inimigo destruindo seus ninhos e ovos no solo do que caçar os pássaros no ar”.² Sua observação continua sendo verdadeira, como demonstrou o ataque mencionado acima. De fato, bases aéreas mal defendidas continuarão a ser suscetíveis à agressões terrestres organizadas. Anteriormente, o ataque mais bem sucedido contra base aérea após Vietnã ocorreu durante a guerra civil do El Salvador em 1982, na qual 100 insurgentes atacaram uma base aérea salvadorenha, destruindo cinco aeronaves *Ouragan*, seis *UH-1Bs* e três *C-47s*, danificando outras cinco plataformas. Sem dúvida, essa “operação bem planejada e executada (. . .) demonstrou a superioridade tática” dos insurgentes contra a força de defesa governamental.³

A proteção de bases aéreas e equipamento aeroespacial no futuro será geometricamente mais complexa e cara, devido a difusão

tecnológica, abundância de informação de fontes abertas e o aumento em capacidade inimiga. No futuro veremos que as ameaças tradicionais, tais como ataques aéreos, fogo indireto [*Indirect Fire - IDF*] de foguetes e morteiros e ataque direto de esquadrões suicidas continuarão a fazer parte da ação inimiga. Por conseguinte, devemos examinar as ameaças emergentes que capacitam novos meios de ataque à bases aéreas, inclusive: o desenvolvimento de munição de precisão; a difusão de VANTs; a proliferação de mísseis superfície-ar [*surface-air missiles - SAMs*], lançados de ombro; o aumento de ameaça interna; e outras variáveis de tecnologia avançada. A defesa de recursos aéreos será cada vez mais problemática, face ao espectro de ameaças possibilitadas pela tecnologia e aceleração em ameaça interna. Essa proliferação e aumento tecnológicos oferecerão vantagens a grupos menores.

Sem dúvida, os Militares da Força Aérea devem levar em consideração a grande probabilidade dessas ameaças incipientes e o custo associado, a fim de assegurar a continuidade operacional. Antigamente, em setores de defesa, um soldado e seu fuzil tomavam conta do recado. As bases aéreas bem defendidas fazem com que o inimigo explore meios alternativos. Naturalmente, após selecionar o alvo, todo protagonista inteligente busca o meio mais barato e rápido para alcançar sucesso. Caso não tente um ataque espetacular, a fim de causar grandes baixas e cobertura dramática pela mídia (como o *Al-Qaeda*), tenta impedir as operações aéreas, sangrando a base aos poucos e produzindo baixas com o passar do tempo.

No entanto, quando examinamos a ameaça, a pergunta sempre deve ser: Qual é o alvo – porque nem sempre trata-se das aeronaves no solo. Os alvos e objetivos dependem daqueles que atacam – grupos terroristas, forças convencionais, operações especiais, que também dependem dos objetivos políticos e da capacidade que conseguem mobilizar.

As forças inimigas descobriram que os ataques em campos aéreos (Vietnã) resultavam em perda de recursos. Assim, adaptaram-se à situação, interrompendo as operações aéreas em lugar de ataque direto aos campos porque “se as incursões danificavam aeronaves, dependências ou pistas, impediam o número de surtidas.

Desde a década de 1960, as armas inatingíveis [*standoff weapons*], atualmente denominadas *IDF*, bem como as várias formas de explosivos

detonados sob comando, rapidamente passaram a ser as armas preferidas dos diversos grupos.⁴

Quanto às operações de defesa de bases, a ameaça terrorista obrigou a mudança de enfoque, ou seja, o combate aos dispositivos explosivos improvisados embarcados [*vehicle-borne improvised explosive devices VBIED*]. Os grupos mais sofisticados colocam à prova ataques que serão divulgados em grandes manchetes, com imagens vívidas, chocantes e baixas de grande impacto. As imagens dos quartéis dos Fuzileiros Navais em Beirute, Líbano e das Torres Khobar, Força Aérea, em Dhahran, Arábia Saudita simbolizam o objetivo dos adversários. Notamos a mesma situação na detonação de caminhão-bomba pelo Talibã no décimo aniversário dos ataques terroristas de 11 de setembro de 2001—um golpe que resultou em 89 feridos, inclusive 77 Soldados.⁵

Este artigo examina algumas das ameaças mais alarmantes—tais como *VBIEDs*, que o inimigo provavelmente utilizará em futuros ataques—e a tecnologia emergente que capacitaria o mesmo a assediar nossas bases.

A Precisão Cada Vez Maior do Fogo Indireto

O *IDF* é a opção preferida dos insurgentes. Frequentemente armado para disparar após a partida do protagonista, à distância, oferece certo grau de sobrevivência.

Décadas antes, o Vietcong e as forças nortevietnamitas atacaram as bases aéreas norteamericanas 475 vezes entre 1964 e 1973, especialmente com *IDF*, destruindo 99 aeronaves norteamericanas e sulvietnamitas e danificando 1.170.⁶

No Iraque, os insurgentes utilizaram *IDF* para assediar as bases aéreas. Contudo, foi algo ineficaz, devido a um inimigo mal treinado e defesas externas dinâmicas.

No Afeganistão o inimigo empregou *IDF* não só para assediar as forças de coalizão mas também para encobrir e disfarçar ataques

terrestres. No dia 22 de agosto de 2012, forças inimigas conseguiram, até mesmo, danificar a aeronave dos Chefes do Estado Maior em visita oficial.⁷

Os morteiros e foguetes em mãos de indivíduo com dados limitados do alvo, dependem da perícia técnica do operador—o que impede a eficácia geral. Contudo, o advento de nova era em precisão de sistemas *IDF* mudou o cenário. No dia 31 de março de 2011, os Soldados da Equipe de Combate da Quarta Brigada [*4th Brigade Combat Team*] dispararam um morteiro de precisão, teleguiado de 120 mm, da Base de Operações Avançadas Kushamond [*Forward Operating Base Kushamond*], Afeganistão, chegando a quatro metros do alvo.⁸ Normalmente um morteiro dispara um tiro de ensaio [*“dumb” round*]—que não possui sistema teleguiado embarcado. Com o passar do tempo a nova tecnologia provavelmente será difundida entre os grupos insurgentes e terroristas, aperfeiçoando sua habilidade em seleção de alvos, resultando em extraordinária precisão, fazendo com que as aeronaves e dependências principais fiquem ainda mais vulneráveis.

A derrota desse tipo de sistema de armas exige defesa tecnológica verdadeiramente integrada. Os Estados Unidos e Israel foram os pioneiros em sistemas de defesa projetados para combater a precisão cada vez maior de armas *IDF*.

A Base Conjunta Balad e outros locais empregaram um sistema de Morteiro de Artilharia de Combate a Foguetes [*Counter-Rocket Artillery Mortar*] para defender contra *IDFs* no Iraque.

O Departamento de Defesa deverá assegurar a existência de sistema de defesa no futuro, porque a munição de precisão fará com que os ataques sejam bem mais simples, proporcionando às forças de defesa menor margem de erro. Além disso, a capacidade dessa tecnologia de defesa está ficando cada vez melhor. Por exemplo, durante o conflito de Israel contra Hamas em Gaza em novembro de 2012, os militantes lançaram mais de 1.500 foguetes em Israel, mas a Cúpula de Ferro [*Iron Dome*] daquele país, um “sistema portátil anti-foguetes projetado para abater mísseis de curto alcance” interceptou cerca de 400.⁹ Pode ser que esse sistema sirva de modelo para sistemas de defesa em operações aéreas. Se as munições de precisão *IDF* passarem a fazer parte do ambiente operacional, os Militares da Força Aérea não poderão se dar ao

luxo de depender da incompetência de um inimigo que dispara tiros de ensaio.

VANTs

O pessoal encarregado da defesa de bases aéreas deve considerar a ameaça que os VANTs apresentam, formulando plano para reagir à ameaças remotas, tanto terrestres como aéreas. Quem está autorizado a engajar esses veículos e com que tipos de arma. Para veículos terrestres define-se a ameaça com maior clareza e de conformidade com as contingências estabelecidas para os *VBIEDs*. No entanto, pode ser que exista uma lacuna defensiva em defesa de ameaças aéreas. O fato de que ainda resta explorar completamente os protocolos para essas defesas deixa uma falha que inimigos tecnologicamente inteligentes podem explorar.

Devemos desenvolver modelos, simulações e defesas para cobrir essas novas ameaças antes que grupo interrompa as operações de voo ou—pior ainda—antes que organização terrorista utilize VANTS para reconhecimento ou investidas contra nossos recursos aéreos.

O uso desses veículos [Em Inglês o termo *drone*=robô significa todo veículo remotamente pilotado, quer seja aéreo, terrestre ou marítimo], já ultrapassa o uso militar exclusivo. Afinal de contas, a população civil opera aeroplanos via controle remoto desde a década de 30. Agora, no entanto, a sofisticação, alcance e capacidade videográficas permitem à população civil acesso à tecnologia antes reservada somente ao emprego militar e organizações secretas. Consideremos o caso de um grupo de protesto denominado *SHARK* (*Showing Animals Respect and Kindness* – Respeito e Benevolência para com os Animais). Esse grupo planejou o uso de *Mikrokopter* para videografar caçadores que disparavam contra pombos, a fim de dissuadir e interferir com caçada legítima. No dia 21 de fevereiro de 2012, o *SHARK* estabeleceu operações na Plantação de *Broxton Bridge* próximo a Ehrhardt, Carolina do Sul. Os agentes de ordem pública e um advogado da localidade tentaram bloquear o grupo e impedir a filmagem, mas não conseguiram. Os caçadores acabaram atirando e abatendo o helicóptero no local.¹⁰

Essa mesma tecnologia é capaz de portar armas e levar a cabo reconhecimento para grupos que têm como alvo um campo de pouso—de

fato, já o fizeram. Por exemplo, embora as autoridades competentes dos E.U.A. preocupem-se com o *Al-Qaeda*, o *Hezbollah* (Partido de Allah) comprovou que possui alcance e resistência globais. Foi o primeiro grupo terrorista a utilizar pessoas com coletes explosivos como arma de destruição em massa, transportando grandes veículos bombas a alvos específicos.¹¹ O *Hezbollah* recentemente demonstrou conhecimento tecnológico com o uso de VANTs repletos de explosivos, bem como mísseis, conseguindo até mesmo incapacitar um navio de guerra israelita.¹² Deve-se o sucesso da organização ao respaldo financeiro e logístico da Síria e Irã, esse último suprindo armamento avançado e equipamento de reconhecimento.

Com início em novembro de 2004, o *Hezbollah* chocou os israelitas ao lançar avião de vigilância remotamente pilotado, o *Mirsad 1*, que sobrevoou cidades israelitas e regressou ao Líbano ileso. Durante um comício do *Hezbollah*, o líder, Hassan Nasrallah, declarou, “Pode-se carregar o *Mirsad* com 40 - 50 quilos de explosivos e enviá-lo ao alvo (. . .) Quer seja usina elétrica, hidráulica, base militar – não importa o que!”¹³ Sem dúvida essa tecnologia estará disponível a outros terroristas e grupos com o passar do tempo.

A fim de destacar esse ponto, vejamos o caso de Rezwan Ferdaus, um cidadão norteamericano de 26 anos de idade. Foi apreendido no dia 28 de setembro de 2011, acusado de planejar os ataques contra o Pentágono e o Capitólio em WA D.C. com “grande aeronave controlada remotamente, repleta de plástico explosivo C-4”, bem como providenciar “material de apoio e recursos à organização terrorista estrangeira, especificamente, *Al Qaeda*.”¹⁴ De acordo com o *Federal Bureau of Investigation*, Ferdaus planejava combinar o “ataque aéreo” com três robôs carregados de explosivos e ataque terrestre que incluía “seis pessoas com armas de fogo, automáticas, divididas em duas equipes”. Ferdaus explicou que “com este ataque aéreo, efetivamente eliminamos pontos essenciais do edifício P [Pentágono] e depois aumentamos o dano, a fim de destruir o restante, deixando somente uma área de engarrafamento onde os indivíduos ficarão isolados, vulneráveis [para que] possamos dominar”.¹⁵

A Proliferação de Mísseis Superfície-Ar, Lançados de Ombro

Uma ala voadora consegue alcançar êxito somente com surtidas aéreas, não importa a ameaça do ambiente operacional. A proteção de aeronaves durante a decolagem, a fase mais vulnerável do voo, é extremamente difícil, devido as restrições de manobrabilidade causadas pelo peso e baixa altitude. Consequentemente, as aeronaves de transporte pesado e suas cargas valiosas, como munição e/ou passageiros, oferecem alvos extremamente atraentes durante a decolagem (*SAMs*). As aeronaves que se aproximam à aterrissagem estão chegando ao final do combustível e devem manter velocidades e rotas previsíveis. Em qualquer um desses casos, os *SAMs* preocupam. Por exemplo, os rebeldes no conflito atual na Síria supostamente possuem cerca de “quinze a trinta sistemas portáteis de defesa aérea SA-7 [*man-portable air-defense systems - MANPADS*]” e “presumivelmente abateram, no mínimo, cinco aeronaves de asa giratória e seis de asa fixa”, alegando, pelo menos, uma abatida via *MANPADS*.¹⁶ De acordo com o Centro de Combate à Proliferação da Força Aérea dos E.U.A. [*US Air Force Counterproliferation Center*]:

Atualmente, 27 grupos terroristas, inclusive o *Al Qaeda*, confirmaram ou relataram a posse de *MANPADS*. Desde 1994, dez atentados de alto perfil, tendo em mira aeronaves de linhas aéreas comerciais, quatro abatidas – inclusive uma que transportava os Presidentes da Ruanda e de Burundi. Além do mais, os *MANPADS* encaixam-se perfeitamente bem ao modo de operação de *Al Qaeda*, são relativamente fáceis de usar e transportar, amplamente disponíveis, não dispendiosos e, sem dúvida, letais.¹⁷

À medida que a tecnologia desenvolvida pelos competidores estrangeiros continua a avançar e a proliferar, as táticas, técnicas e procedimentos para a defesa integrada terá que se manter em dia com seu emprego. Recentemente, o *MANPADS* russo SA-24 “*Grinch*” foi enviado à Venezuela, Líbia e Síria.¹⁸ É claro que o governo da Líbia foi deposto e a Síria continua em pé de guerra. A segurança de *MANPADS* em tais países permanece em dúvida, à medida que surgem possíveis mercados negros e a instabilidade atrai elementos nefários. A ameaça de *MANPADS* às futuras forças norteamericanas e de coalizão, bem como às operações de linhas aéreas civis provavelmente aumentará, à medida que esses sistemas ficam mais acessíveis em solo fértil à guerras civis e insurgências.

O Aumento da “Ameaça Interna”

Em futuro previsível, as forças norteamericanas e de coalizão operarão dentre ameaças internas. No Afeganistão, de 2007 a 2011, as estatísticas do Pentágono revelaram um total de 42 ataques pelos membros das Forças de Segurança Nacional do Afeganistão [*Afghan National Security Forces*] contra pessoal norteamericano e da OTAN, com a perda de vida de 70 tropas da coalizão e ferindo 110 outros.¹⁹ Um dos exemplos mais flagrantes e horrendos de ameaça interna ocorreu na manhã de 27 de abril de 2011, quando um capitão da Força Aérea Afegã matou oito Militares da Força Aérea e um empreiteiro no Aeroporto Internacional de Cabul.²⁰ Outro incidente demonstrou como um suicida determinado e astuto conseguiu infiltrar uma base da *Central Intelligence Agency* no leste do Afeganistão, eliminando oito norteamericanos.²¹ Essa tendência alarmante intensificou em 2012, à medida que as forças de segurança afegãs uniformizadas levaram a efeito 46 ataques internos contra as forças da coalizão, executando 60 membros da OTAN.²²

O que mais inquieta é a ameaça, cada vez maior, que ocorre dentro das forças armadas norteamericanas. No dia 11 de maio de 2009, cinco membros das forças armadas norteamericanas foram assassinados por um Soldado dos E.U.A. em um centro de terapia militar no *Camp Liberty*, Bagdá.²³

O tiroteio levado a efeito por um psiquiatra do Exército dos E.U.A. no dia 5 de novembro de 2009 em Fort Hood, Texas, resultou em morte de 13 pessoas, ferindo outras 32.²⁴ Sem dúvida, o Departamento de Segurança do Território Nacional [*Department of Homeland Security*] está apreensivo com a ameaça apresentada pelos veteranos, notando que os membros das forças armadas que regressam do Iraque e do Afeganistão podem ser suscetíveis a recrutamento por extremistas da extrema direita.²⁵

É importante lembrar que uma só pessoa consegue causar grande dano—considerem o número de incidentes causados por “lobos solitários”. Por exemplo, no dia 22 de julho de 2011, Anders Breivik, um norueguês, explodiu um veículo-bomba próximo a edifícios governamentais em Oslo, matando oito e, mais tarde, massacrando 69

pessoas em um acampamento de jovens na ilha de Utoeya próxima ao local.²⁶ No dia 20 de julho de 2012, o norteamericano James Holmes entrou em um cinema superlotado nos subúrbios de Denver, Colorado e começou a disparar. Matou 12 e feriu 58.²⁷ Os membros das forças armadas norteamericanas treinados e experientes, bem como veteranos podem causar ainda maior destruição. Quer seja no território nacional ou estrangeiro, os comandantes devem assegurar-se de que proporcionam e colocam em funcionamento um plano de segurança interna bem compreensivo—inclusive um programa de triagem psicológica dinâmico, a fim de identificar esse tipo de ameaça.

Acesso a Mapas

As forças inimigas que planejavam investidas terrestres de bases aéreas costumavam basear-se em colaboradores com acesso à mesma, a fim de facilitar o mapeamento do terreno e o local específico de dependências principais, bem como obter a contagem de passos [necessários para alcançar dado local] o que tornava possível os golpes via *IDF*. Atualmente, a Internet oferece acesso à imagens via satélite e outros dados que tornam a tarefa de futuro agressor bem mais fácil. Um local, o da Federação de Cientistas Americanos [*Federation of American Scientists – FAS*] descreve sua organização: “laboratório de ideias independente, não filiado e organização registrada, sem fins lucrativos [501(c)(3)] (. . .) dedicada a providenciar análise rigorosa, objetiva e baseada em provas e recomendações de diretrizes práticas para questões relacionadas à segurança nacional e internacional, à ciência aplicada e à tecnologia”.²⁸ A *GlobalSecurity.org*, organização derivada desta última, fundada por John Pike, um de seus antigos membros, declara ser “a fonte líder em dados fundamentais, gerando relatórios em áreas de defesa, espaço, inteligência, *WMD* [*weapons of mass destruction*] e segurança do território nacional”.²⁹ Sua página da *Internet* contém imagens de satélite de bases militares ao redor do mundo, muitas delas restritas. Outras, tais como *Google Maps*, colocam à disposição imagens e mapas de sistemas rodoviários. Em suma, existem agora inúmeros meios de aquisição de mapas detalhados de bases aéreas que facilitariam as investidas.

Os Meios Sociais:

Flash Mobs, Terrorismo e Ataques de Redes

A comunicação instantânea dramaticamente aperfeiçoará as operações de informática do inimigo e seus ataques, permitindo o recrutamento de simpatizantes dentre a população local, a fim de criar situações que embaraçam a liderança das bases ou superam suas defesas. Assim, as organizações dedicadas à inteligência e à ordem pública devem estar sempre um passo à frente de um inimigo cada vez mais ágil. Devem ser mais hábeis em suas tentativas de compilação de dados. A tecnologia básica, tais como telefones celulares, afetou a sociedade de maneira fora do comum, criando meios inéditos de comunicação e de ações coordenadas. Vejamos, por exemplo, o fenômeno de “*flash mobs*”, um grupo de pessoas convocado via celular, *social media* e correio-eletrônico para o propósito de desempenhar algum tipo de peça teatral em local específico. A *Internet* e até mesmo empresas de telecomunicações estão repletas de gravações de grupos que aparecem em público para desempenhar peças artísticas, como números de dança, árias e concertos. Embora seja para puro entretenimento, o que acontece se alguém utiliza essa mesma tática para propósitos nefários?

No verão de 2011, por exemplo, a Filadélfia foi assolada por verdadeira epidemia de *flash mobs* organizadas para praticar roubos, assaltos, pilhagens e causar caos. Incluía a agressão de pedestres, uma corrida desenfreada pela loja *Sears* e a reunião de centenas de pessoas em locais designados com o propósito de engarrafar o trânsito. Margaret Rock, editora da *Multimedia.com* em Chicago, disse o seguinte: “Não sei por que, mas aquilo que começou como algo de bom está agora revelando seu lado mau”.³⁰ Mais tarde, naquele mesmo Verão, distúrbios em Londres, Birmingham, Manchester e outros locais causaram grande problema às autoridades encarregadas de segurança. A *Scotland Yard* identificou e prendeu cerca de 3.000 pessoas suspeitas (participação física em tumultos ou incitação à violência) que utilizaram o *BlackBerry Messenger*, *Twitter* e *Facebook*.³¹ De acordo com um texto: “Se quiser ganhar dinheiro, estamos a ponto de dar duro no Leste de Londres”.³² David Cameron, o Primeiro-Ministro da Grã-Bretanha observou que “todos aqueles que presenciam essas ações terríveis ficarão chocados em saber que foram organizadas via *social media* (. . .) Assim, estamos colaborando com a polícia, as agências de inteligência e a indústria para ver se seria possível fazer com que as pessoas não consigam comunicar-

se através desses *sites* e serviços, quando sabemos que estão planejando violência, desordem e criminalidade”.³³

O ritmo acelerado do avanço tecnológico difundiu-se a todos os cantos da Terra. Os celulares são agora poderosos computadores em si, comunicando-se com outros dispositivos em todas as partes. Isso se torna bem aparente em países em fase de desenvolvimento que possuíam péssima comunicação, devido a falta de infraestrutura necessária para as linhas terrestres, agora obsoletas, porque as torres e satélites permitem a tais países conectar-se com a rede global. Desde 2008, 80 por cento da população mundial possui acesso à rede celular e ao final de 2006, os países em desenvolvimento compraram 68 por cento dos celulares existentes.³⁴

A mesma tecnologia que capacita a partilha mundial de dados também apoia a comunicação entre terroristas e grupos delinquentes. De acordo com novo estudo feito pela Universidade de Haifa em Israel, *Al-Qaeda, Hamas, Hezbollah* e outros semelhantes investiram em *social networking* tais como *Facebook* e *Twitter*, a fim de recrutar, angariar fundos e inteligência. O Prof. Gabriel Weimann, autor do estudo, alega que “hoje, cerca de 90 por cento do terrorismo organizado na *Internet* está sendo transmitido pela *social media*” e que essa última “capacita as organizações terroristas a tomar iniciativas, solicitando ‘amigos’, baixando vídeos e outros dados. Não mais são relegados a subsistir com os dispositivos passivos disponíveis em *sites* normais”.³⁵

Como será que essa tecnologia e comunicação em rede afetará a segurança de bases no futuro? Os dissidentes, grupos rebeldes terroristas podem facilmente ser convocados sem que a inteligência militar ou a ordem pública receba notificação prévia, reunindo-se rapidamente próximo à entrada da base ou perímetro para protestar, causar distúrbios ou atacar. Em muitas ocasiões, tais áreas contam somente com um punhado de guardas disponíveis para combater os grupos em massa—um cenário que pode facilmente superar o pequeno número de pessoal no local e escalar além de sua capacidade de combater tal ação.

Ataque Cibernético: Possivelmente um “Botão de Fácil Acesso” ao Ataque

Os avanços tecnológicos impulsionaram as forças armadas norte-americanas, transformando-as em “força cibernética”. Dependem, em grande parte, de rede de computadores e vínculos de comunicação para assegurar, não só o uso eficaz de forças durante operações de contingência, mas também a missão cotidiana de prontidão e treinamento da força. Até agora, as forças insurgentes não possuíam a capacidade e o treinamento para levar a cabo ataques cibernéticos em grande escala contra instalações militares. No entanto, isso provavelmente irá mudar, à medida que as organizações terroristas patrocinadas pelas nações e as forças insurgentes entram em parceria para derrotar inimigo comum.

A utilização de ataque cibernético para afetar as operações aéreas ou sensores de defesa de base e câmeras para facilitar ataque cinético são opções eficazes pouco dispendiosas.

Os ataques via ciberespaço resultam em operações de voo degradadas, como ocorreu no Aeroporto Internacional de Indira Gandhi, quando um código malicioso, utilizando notação especificamente projetada para explorar os pontos fracos daquele sistema, fechou os balcões de entrada e os portões de embarque, quase que por completo afetando as operações.³⁶ Agressão similar interromperia os centros de controle de tráfego aéreo, redes de escalas de manutenção e operações de treinamento, bem como ameaçaria VANTs, armados ou não, operados pela Força Aérea e outras agências governamentais. Vejamos, por exemplo, a aposta entre um Catedrático universitário do Texas e seus alunos – que acabou levando ao recente *hacking* de robô do Departamento de Segurança do Território Nacional [*Department of Homeland Security*]. Por menos de \$1.000,00 dólares esses indivíduos foram bem sucedidos em “enganar” o VANT, reprogramando sua missão.³⁷ Essa brincadeira acadêmica barata demonstra como é fácil para adversário ou grupo terrorista reprogramar VANTs transformando-os em mísseis voadores contra suas próprias bases aéreas ou outros alvos.

Red Flag, o exercício de treinamento de combate da Força Aérea no qual participam os Estados Unidos e as forças aliadas, integra os elementos ciberespaciais do Comando Espacial da Força Aérea [*Air Force Space Command*] para tratar dos efeitos associados aos ataques contra

recursos ciberespaciais. No exercício de março de 2011, um oficial da Força comentou: “Sabemos que muitas ameaças ao redor do globo diligentemente tentam obter acesso, corromper e negar nosso uso de sistemas de informática [segredo ou não]”.³⁸ Os recursos e pessoal associados aos sistemas de defesa integrada também podem vir a ser alvos. Além do mais, os adversários podem tentar perturbar ou manipular o aumento cada vez maior em uso do ciberespaço para comunicações, inclusive transmissões de rádio codificadas e restritas e mensagens não restritas, bem como sistemas de identificação biométrica em nossos portões de entrada. Uma investigação do *Washington Post* descobriu que certos tipos de plataformas para programas utilizados pelo governo e setor privado, inclusive um sistema denominado *Niagara* da empresa *Tridium*—são mais vulneráveis do que outros. Marc Petock, o Vice-Presidente da *Tridium*, encarregado do mercado global e comunicações notou que “algumas dependências do Departamento de Defesa nos Estados Unidos também dependem do *Niagara*, inclusive o gigantesco Arsenal do Exército Tobyhanna [*Tobyhanna Army Depot*] em Pensilvânia” e certas dependências militares de “alta segurança”.³⁹

O domínio ciberespacial em rápida evolução promete muitos benefícios: redução em requisitos de mão de obra, aumento em eficiência, melhor seleção de alvos e fácil acesso/uso. No entanto, essa mesma tecnologia oferece grandes oportunidades a adversário esperto e determinado a criar uma porta dos fundos pela qual consegue penetrar e derrotar todo um sistema de segurança.

A Introdução de Tecnologia Moderna nas Forças Especiais

Há pouco tempo, os encarregados de planejamento em bases da OTAN analisaram os planos da União Soviética de ataque as nossas bases aéreas. Durante a Guerra Fria, os soviéticos buscaram inúmeros meios de invadir e incapacitar as bases, especialmente com o emprego de *Spetsnaz* (forças especiais). Uma revisão feita pela *Central Intelligence Agency* dos perfis de ataque a campos de pouso da *Spetsnaz* em relatórios da era da Guerra Fria, agora liberados, seria útil porque ofereceria diferentes perspectivas em métodos de ataques diretos. Essas forças incluem 30 operadores especiais que saltam de paraquedas próximo à base e dividem-se em “quatro equipes, cada qual com responsabilidades específicas, inclusive a captura de veículos e pessoal

com o propósito de infiltrar o objetivo [base aérea]”, utilizando SAMs e dispositivos explosivos para destruir as aeronaves.⁴⁰

Em outro método, um grupo de *Spetsnaz* (aproximadamente 10 equipes de cinco a doze membros) operaram contra campo de pouso altamente defendido. O grupo não conseguiu chegar a menos de 2 - 3 km do objetivo. Durante a primeira noite os *Block Strelas* [três lança-SAMs em tubos, montados em tripé] foram posicionados, o mais próximo possível, nas duas extremidades do campo de pouso, iniciando-se os ataques contra oleoduto, redes elétricas, linhas de comunicação, pessoal de segurança e tripulações que se encaminhavam ao campo de pouso.⁴¹

Isso perturbaria operações aéreas, criaria a impressão de que maior força soviética estaria na área e atrairia maior número de forças da OTAN para a defesa, retirando-as das linhas de frente. Imaginem forças especiais inimigas bem treinadas e apetrechadas com os muitos avanços tecnológicos que acabamos de mencionar. A defesa de base seria incrivelmente difícil e a complexidade de combate à ameaça iria escalar muito mais.

Conclusão

Devemos compreender e combater essas ameaças, o que desempenhará papel principal na habilidade de projetar o poder aéreo de forma eficaz no futuro. Uma das soluções apresentada—abrigar as aeronaves o mais longe possível das hostilidades—causa maior estresse às aeronaves e às tripulações, devido a períodos de voo mais longos. No entanto, não se dirige à probabilidade do requisito de que as aeronaves de transporte de tropas aterrissem próximo a, ou dentro da, zona de combate para apoiar as operações terrestres. As bases remotas tampouco solucionam os meios tecnológicos de ataque ciberespacial, de terroristas capacitados tecnologicamente e de forças especiais que atacam base aérea supostamente segura. Assim, os Militares da Força Aérea devem levar a efeito uma análise de ameaça que abrange verdadeiramente todo o espectro, levando em consideração essas possíveis vulnerabilidades em planejamento de proteção de força.

As aeronaves são extremamente frágeis. Um disparo de morteiro bem posicionado inutiliza várias, ou seja, centenas de milhões de dólares ou completamente destroi dependências militares ocupadas por pessoal essencial, tais como pilotos e técnicos. A Força Aérea e as forças de coalizão deverão tomar decisões bem difíceis acerca de defesa de base, tudo influenciado pelos requisitos de missão, restrições econômicas e a ameaça elevada de inimigos determinados em posse de tecnologia de ponta. Os Militares da Força Aérea e líderes conjuntos devem, ou manter-se à frente dessas questões durante os anos entre guerras, ou arriscar a eliminação e degradação de recursos aéreos no início da próxima campanha acirrada.

Notas

1. Barbara Starr, Chris Lawrence e Joe Sterling, "ISAF: Insurgents in Deadly Attack in Afghanistan Wore U.S. Army Uniforms," Cable News Network, 15 September 2012, <http://www.cnn.com/2012/09/14/world/asia/afghanistan-fatal-attack/index.html>.

2. Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (1942; new imprint, Washington, DC: Office of Air Force History, 1983), 53–54.

3. James S. Corum e Wray R. Johnson, *Airpower in Small Wars: Fighting Insurgents and Terrorists* (Lawrence: University Press of Kansas, 2003), 334–35.

4. Maj Michael P. Buonaugurio, USAF, "Air Base Defense in the 21st Century: USAF Security Forces Protecting the Look of the Joint Vision" (tese de mestrado, Escola de Comando e Estado-Maior dos Fuzileiros Navais [Marine Corps Command and Staff College], 2001), 8, <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA401262>.

5. Jeremy Kelly, "NATO Military Base Attacked by Suicide Bomber in Afghanistan," *Guardian*, 11 September 2011, <http://www.guardian.co.uk/world/2011/sep/11/us-base-suicide-bomber-afghanistan>.

6. Alan Vick, *Snakes in the Eagle's Nest: A History of Ground Attacks on Air Bases* (Santa Monica, CA: RAND, 1995), 68, http://www.rand.org/content/dam/rand/pubs/monograph_reports/2006/MR553.pdf.
7. Barbara Starr, "Shrapnel Hits Joint Chiefs Chairman's Plane at Afghan Base" Cable News Network, 21 August 2012, http://articles.cnn.com/2012-08-21/asia/world_asia_afghanistan-dempsey-plane_1_fight-against-afghan-green-on-blue-afghan-man-afghanistan.
8. SSgt Todd Christopherson, "Soldiers Fire First Precision-Guided Mortar in Afghanistan," US Army, 7 April 2011, <http://www.army.mil/article/54502/>.
9. Jennifer Rizzo, "U.S. Continues Support for Israel's Iron Dome," Cable News Network, 17 May 2012, http://articles.cnn.com/2012-05-17/us/us_israel-missile-system_1_anti-rocket-iron-dome-missile-defense?s=PM:US; and Ernesto Londoño, "For Israel, Iron Dome Missile Defense System Represents Breakthrough," *Washington Post*, 2 December 2012, http://www.washingtonpost.com/world/national-security/for-israel-iron-dome-missile-defense-system-represents-breakthrough/2012/12/01/24c3dc26-3b32-11e2-8a97-363b0f9a0ab3_story_1.html.
10. Rebecca Boyle, "[After Animal Activists Track Pigeon Hunt with Drone, Pigeon Hunters Shoot Down Drone](#)," *Popular Science*, 21 February 2012, <http://www.popsci.com/technology/article/2012-02/after-pigeon-hunt-thwarted-shooters-take-down-activist-groups-spy-drone>.
11. Capt Daniel Helmer, "Hezbollah's Employment of Suicide Bombing during the 1980s: The Theological, Political, and Operational Development of a New Tactic," *Military Review*, July–August 2006, http://www.army.mil/professionalWriting/volumes/volume4/november_2006/11_06_1.html.
12. Associated Press, "Israel: Iranian Troops Helping Hezbollah Attack," *NBC News*, 16 July 2006, <http://www.nbcnews.com/id/13875121/>.

13. Lisa Myers, “Hezbollah Drone Threatens Israel,” *NBC News*, 12 April 2005, <http://www.msnbc.msn.com/id/7477528/ns/nbcnightlynews/t/hezbollah-drone-threatens-israel/>.

14. “Massachusetts Man Charged with Plotting Attack on Pentagon and U.S. Capitol and Attempting to Provide Material Support to a Foreign Terrorist Organization,” comunicado de imprensa, Federal Bureau of Investigation, 28 September 2011, <http://www.fbi.gov/boston/press-releases/2011/massachusetts-man-charged-with-plotting-attack-on-pentagon-and-u.s.-capitol-and-attempting-to-provide-material-support-to-a-foreign-terrorist-organization>.

15. Ibid.

16. Eddie Boxx e Jeffrey White, “Responding to Assad’s Use of Airpower in Syria,” Washington Institute for Near East Policy, 20 November 2012, <http://www.washingtoninstitute.org/policy-analysis/view/responding-to-assads-use-of-airpower-in-syria>.

17. James C. “Chris” Whitmire, *Shoulder Launched Missiles (a.k.a. MANPADS): The Ominous Threat to Commercial Aviation*, Counterproliferation Papers, Future Warfare Series no. 37 (Maxwell AFB, AL: USAF Counterproliferation Center, Air University, December 2006), 1, <http://cpc.au.af.mil/PDF/monograph/manpads.pdf>.

18. David Fulghum e Robert Wall, “Russia’s SA-24 ‘Grinch’ Lands in Insurgent Hands,” *Aviation Week and Space Technology*, 12 March 2012, http://www.aviationweek.com/Article.aspx?id=/article-xml/AW_03_12_2012_p27-433282.xml&p=1.

19. Anna Mulrine, “Taliban Infiltrators in Afghanistan? Pentagon Warns of ‘Insider Threat,’” *Christian Science Monitor*, 1 February 2012, <http://www.csmonitor.com/USA/Military/2012/0201/Taliban-infiltrators-in-Afghanistan-Pentagon-warns-of-insider-threat>.

20. Jill Laster, “Motive in Kabul Shooting Deaths Remains Elusive,” *Air Force Times*, 17 January 2012, <http://www.airforcetimes.com/news/2012/01/air-force-motive-in-kabul-shooting-deaths-remains-elusive-011712/>.

21. Joby Warrick, "Suicide Bomber Attacks CIA Base in Afghanistan, Killing at Least 8 Americans," *Washington Post*, 31 December 2009, <http://www.washingtonpost.com/wp-dyn/content/article/2009/12/30/AR2009123000201.html>.

22. "What Lies behind Afghanistan's Insider Attacks?," British Broadcasting Corporation, 11 March 2013, <http://www.bbc.co.uk/news/world-asia-19633418>.

23. Timothy Williams, "U.S. Soldier Kills 5 of His Comrades in Iraq," *New York Times*, 11 May 2009, http://www.nytimes.com/2009/05/12/world/middleeast/12iraq.html?_r=2.

24. Joseph I. Lieberman e Susan M. Collins, *A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack*, relatório especial (Washington, DC: US Senate Committee on Homeland Security and Governmental Affairs, February 2011), <http://www.hsgac.senate.gov/download/fort-hood-report>.

25. Associated Press, "Homeland Security Leaders Defend Memo on Veterans," *USA Today*, 19 April 2009, http://usatoday30.usatoday.com/news/washington/2009-04-19-homeland-memo_N.htm.

26. "Anders Breivik Describes Norway Island Massacre," BBC, 20 April 2012, <http://www.bbc.co.uk/news/world-europe-17789206>.

27. M. Alex Johnson e Pete Williams, "Cops: Weeks of Planning Went into Shootings at Colo. Batman Screening," *NBC News*, 20 July 2012.

28. "About FAS," Federation of American Scientists, acessado em 29 de janeiro de 2013, <https://www.fas.org/about/index.html>.

29. "Company History," GlobalSecurity.org, acessado em 13 março de 2013, <http://www.globalsecurity.org/org/overview/history.htm>.

30. John Timpane, "Flash-Mob Violence Raises Weighty Questions," *Philly.com*, 14 August 2011,

http://articles.philly.com/2011-08-14/news/29886718_1_social-media-flash-mob-facebook-and-other-services.

31. Neil Lancefield, “3,000 Arrests in London Riots Investigation,” *Independent*, 7 October 2011, <http://www.independent.co.uk/news/uk/crime/3000-arrests-in-london-riots-investigation-2366933.html>.

32. Timpane, “Flash-Mob Violence.”

33. Josh Halliday, “David Cameron Considers Banning Suspected Rioters from Social Media,” *Guardian*, 11 August 2011, <http://www.guardian.co.uk/media/2011/aug/11/david-cameron-rioters-social-media>.

34. Sara Corbett, “Can the Cellphone Help End Global Poverty?,” *New York Times*, 13 April 2008, <http://www.nytimes.com/2008/04/13/magazine/13anthropology-t.html?pagewanted=all>.

35. “Terrorist Groups Recruiting through Social Media,” Canadian Broadcasting Corporation News, 10 January 2012, <http://www.cbc.ca/news/technology/story/2012/01/10/tech-terrorist-social-media.html>.

36. Rahul Tripathi, “Cyber Attack Led to IGI Shutdown,” *Indian Express*, 25 September 2011, <http://www.indianexpress.com/news/cyber-attack-led-to-igi-shutdown/851365/>.

37. “Texas College Hacks Government Drone in Front of DHS,” Autonomous Nonprofit Organization (“TV-Novosti”), 27 June 2012, <http://rt.com/usa/news/texas-1000-us-government-906/>.

38. TSgt Scott McNabb, “Red Flag Cyber Operations: Part I—Isn’t Red Flag a Flyer’s Exercise?,” Air Force Space Command, 1 March 2011, <http://www.afspc.af.mil/news/story.asp?id=123244481>.

39. Robert O’Harrow Jr., “Tridium’s Niagara Framework: Marvel of Connectivity Illustrates New Cyber Risks,” *Washington Post*, 11 July 2012, <http://www.washingtonpost.com/investigations/tridiums-niagara->

framework-marvel-of-connectivity-illustrates-new-cyber-risks/2012/07/11/gJQARJL6dW_story.html.

40. Director of Central Intelligence, *Warsaw Pact Nonnuclear Threat to NATO Airbases in Central Europe*, NIE 11/20-6-84, 25 October 1984, 35,
http://www.foia.cia.gov/sites/default/files/document_conversions/89801/DOC_0000278545.pdf. O documento foi agora liberado.

41. *Ibid.*, 36, 39.