ecsbdefesa.com.br
História Militar, Defesa, Estratégia, Inteligência e Tecnologia

OS DRONES E A SEGURANÇA DE DIGNITÁRIOS

Vinícius Domingues Cavalcante, especialista em segurança de dignitários e é Diretor da Associação Brasileira de Profissionais de Segurança – ABSEG (**www.abseg.org.br**)

Nos dias que se seguem, o emprego dos veículos aéreos não tripulados se constitui, ao mesmo tempo, numa ferramenta inestimável para a proteção de autoridades, como também numa das maiores dores de cabeça para os planejadores da segurança desses mesmos dignitários, como excepcionais vetores para atentados.

A tecnologia de aeronaves militares remotamente pilotadas remonta aos anos trinta do século XX. Inicialmente empregados como rebocadores de alvos aéreos para artilharia no solo e posteriormente para tiro de outros aparelhos em vôo, aviões guiados remotamente foram (e são até hoje) também empregados como os próprios alvos e até como projéteis guiados (transportando uma carga explosiva); contudo seu aperfeiçoamento permitiu às forças armadas e de segurança (pública e privada), contarem com uma ferramenta de múltiplas possibilidades de emprego. Os drones podem ser divididos em categorias básicas: Micros, até 2kg de peso; Minis, até 7kg de peso; Pequenos, até 25kg, Médios, até 150kg e Grandes, pesando mais de 150kg. De acordo com seu tamanho, tais aeronaves podem ser equipadas com diversos tipos de sensores, como câmeras de monitoramento de vídeo, com zoom e visão noturna, radares, equipamentos para captação de sinais de rádio/telefonia (ELINT), geração de interferência eletrônica (jamers) etc.

Os Drones, mais conhecidos no Brasil pela sigla de VANT (Veículos aéreos não tripulados) ou ARP (aeronave remotamente pilotada), podem desempenhar, com vantagem e um custo sensivelmente baixo, missões que anteriormente demandariam o emprego de aviões ou helicópteros. Empregando asas fixas (no formato de pequenos aviões ou asas delta) ou asas giratórias (como pequenos helicópteros, com um ou vários rotores), tais aparelhos, movidos por motores elétricos, de combustão interna ou micro-turbinas à jato, possuem diferentes tamanhos e pesos. Há aeronaves minúsculas como a Black Hornet, da Prox Dynamics norueguesa, que pesam incríveis 18 gramas e voam por até 25 minutos, até aeronaves maiores como o Heron,

fabricados pela Israel Aerospace Industries e operados pela Força Aérea Brasileira, de 1.150 kg de peso, com 8,5 metros de comprimento, 16,6 metros de envergadura, com uma autonomia de voo de 37horas.

Há países como Israel, que produzem drones pequenos empregados prioritariamente em vigilância, os quais podem, se necessário, vitimar pessoas e destruir alvos não blindados, atingindo-os de forma velada com uma eficaz carga explosiva de 350g. O drone Spike Firefly, elétrico, pesa 3kg e pode ser facilmente operado por um único soldado, de dia ou a noite, com baixa assinatura visual ou acústica, com alcance de 500m em área urbana e uma autonomia de voo de 15 minutos. Equipamentos como esse podem ser empregados em atentados.

Desde outubro de 2001, na primeira noite da invasão do Afeganistão, drones vem sendo empregados pelos norte-americanos como vetores de ataque, com mísseis e bombas guiadas. Atualmente, os Estados Unidos vem usando drones armados intensamente no Oriente Médio, como recursos em suas campanhas contra a al-Qaeda e o grupo autointitulado Estado Islâmico. Circulando seus alvos a uma altitude em que não podem ser vistos ou ouvidos do solo, aeronaves como o Predator e o Reaper têm sido usados de forma muito bem sucedida contra alvos na Síria, Iraque, Líbia e Iêmen, sendo tais funções de ataque a atribuição mais temível e mais discutida desses equipamentos. Dotados de sofisticadas câmeras de vigilância diuturnas e equipamentos de pontaria a laser, as próprias aeronaves podem localizar os alvos, destruí-los com seu armamento guiado, ao mesmo tempo em que transmite as imagens dos ataques em tempo real para seus operadores que podem até estar em território norte-americano..

Embora normalmente utilizados no ataque a alvos clandestinos, guerrilheiros ou terroristas, em 2 de janeiro de 2020 empregou drones MQ-9 Reaper num ataque a um aeroporto em Bagdá, matando o general iraniano Qasem Soleimani, tido como uma das lideranças mais poderosas do país persa, depois do próprio aiatolá Khamenei. Soleimani, de 62 anos, liderou as operações militares iranianas no Oriente Médio como comandante da Força Quds, unidade de elite da Guarda Revolucionária do Irã. Ele foi morto por mísseis quando sua comitiva deixava o aeroporto, junto a integrantes de uma milícia iraquiana aliada do Irã, em um bombardeio ordenado pelo presidente dos EUA, Donald Trump. Teria sido a primeira vez que drones foram empregados por americanos no ataque a altos dignitários de outro país soberano e um comunicado do Pentágono justificou o ataque afirmando que o general Soleimani "estava desenvolvendo ativamente planos para atacar diplomatas e militares americanos no Iraque e em toda a região".

Em todo mundo, além das forças armadas, as forças de segurança também estão se mobiliando com drones. As polícias se beneficiam dos drones como um instrumento que substitui as dispendiosas aeronaves convencionais (sobretudo os helicópteros) em tarefas como a vigilância discreta de locais, de pessoas, de veículos ou de qualquer tipo de atividade ilegal; atuam como ferramenta de comando e controle em operações em áreas de risco; em operações de contra terror e resgate de reféns; no acompanhamento de multidões no âmbito da segurança de eventos e no controle de distúrbios; na identificação de suspeitos; no monitoramento de tráfego viário; na busca de pessoas desaparecidas em terra e mar; na vigilância de fronteiras e até em acidentes com contaminantes físicos e ambientais.

O Exército dos Estados Unidos iniciou o desenvolvimento de um sistema experimental de armas robóticas (Autonomous Rotorcraft Sniper System – ARSS) em

2005. Testes do equipamento podem ser encontrados na internet; contudo, nenhuma informação sobre o status do sistema foi tornada pública desde 2010. O ARSS consistia em um rifle de precisão acoplado a um pequeno helicóptero autônomo não tripulado e foi planejado para uso em combate urbano ou para várias missões específicas que requeiram atiradores de precisão. O fuzil, um RND Manufacturing Edge 2000 semiautomático disparando o cartucho .338 Lapua Magnum, foi montado em uma plataforma estabilizada, que foi fixada na parte inferior de um drone Vigilante 502. O helicóptero deveria ser pilotado por um piloto automático enquanto um controlador humano apontava e disparava o rifle, que pode disparar até dez tiros certeiros por minuto. A plataforma do armamento, chamada de plataforma de armas de precisão (PWP), foi projetada pelo Laboratório de Dinâmica Espacial da Universidade do Estado de Utah e foi equipada com uma câmera de percepção situacional e um escopo de zoom de dois níveis. O sistema usou muito hardware comercial disponível para reduzir custos e tempo de desenvolvimento. Por exemplo, o sistema foi controlado usando um controlador de videogame Xbox 360. Outras armas consideradas para uso com o ARSS incluíam as metralhadoras M249 ou M240, a espingarda AA-12 ou armas não letais. Em 2006, Neural Robotics Incorporated (NRI), de Huntsville, Alabama, apresentou a versão armada do mini helicóptero não tripulado AutoCopter às forças de segurança. A aeronave pilotada remotamente dispunha de uma espingarda automática de calibre 12, AA-12 e podia disparar diversos tipos de projéteis, letais e não-letais.

No Brasil a plataforma de governo de um governador do estado do Rio de Janeiro veiculava a aquisição de drones armados para abater criminosos armados de fuzis encastelados em favelas, com o mínimo de dano colateral. Embora atualmente, diversas empresas já vem oferecendo aeronaves remotamente pilotadas multi-rotor, equipadas com armas de fogo para propósitos de segurança, tanto para escolta, quanto para eliminação física específica de ameaças criminais, infelizmente, tal solução para enfrentar criminosos fluminenses ficou apenas no campo da retórica de campanha eleitoral. Embora não tenhamos conhecimento específico de instituições

que tenham adotado tais equipamentos, certamente, tais equipamentos fabricados industrialmente já devem estar disponíveis para uso em diversos países.

Na segurança de autoridades, um ou mais drones de vigilância podem ser empregados tanto no reconhecimento das áreas onde dignitários terão de ingressar (inclusive para identificação de pessoas, veículos ou objetos suspeitos), quanto no comandamento panorâmico de eventos pelos encarregados da sua segurança pessoal no local.

O USO ADVERSO DAS AERONAVES REMOTAMENTE PILOTADAS

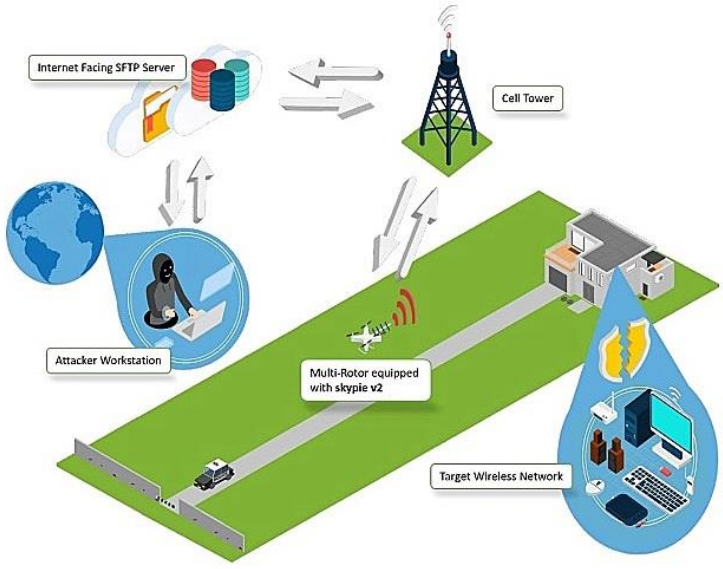
A enorme proliferação dessas aeronaves remotamente pilotadas também agrava os riscos para a segurança personalidades e de instalações. A possibilidade do emprego criminoso desses engenhos é hoje uma realidade. Na verdade, assim como ocorre com os artefatos explosivos improvisados, a adaptação de drones para ações criminosas e terroristas é algo que apenas será limitado pela capacidade inventiva e dos recursos técnicos postos à disposição de seus projetistas/usuários.

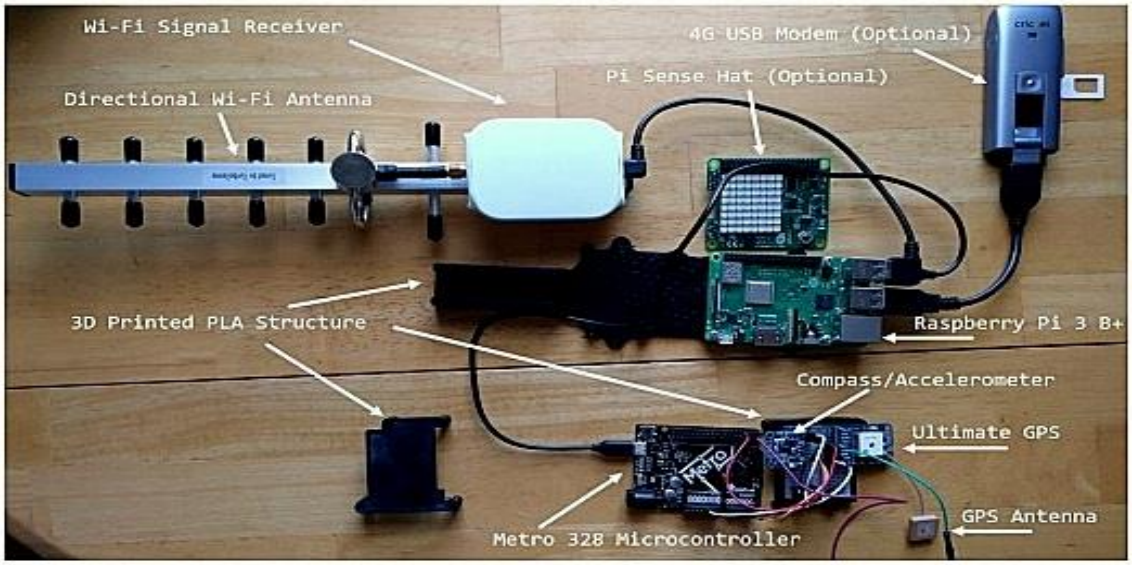
Drones podem ser empregados para espionar instalações, pessoas e o que acontece em seu interior. São costumeiramente usados para contrabandear telefones celulares, armas e drogas para estabelecimentos prisionais. Já foram empregados para perturbar eventos esportivos, como em setembro de 2016, no US Open, quando um drone voou ao redor da quadra de tênis antes de bater na área do campo e provocar a temporária interrupção da partida. Em maio de 2015, quando fazia um grande show em Tijuana, no México, o cantor espanhol Enrique Iglesias agarrou um pequeno ARP que filmava a sua apresentação e por pouco não perdeu os dedos.

Dotar drones com armas de fogo também é algo que também pode ser feito clandestinamente. Um jovem estudante de engenharia de Connecticut, de 18 anos, chamado Austin Haughwout postou na internet um vídeo que mostra tiros sendo disparados de um drone armado com uma pistola em julho de 2015. O vídeo acumulou mais milhões de visualizações no Youtube e Whatsapp e gerou uma investigação da Agência Federal de Aviação dos Estados Unidos (FAA).

Aeronaves remotamente pilotadas também podem ser utilizadas para sabotar instalações ou atingir pessoas, disseminando de agentes químicos ou biológicos. Manifestantes japoneses adaptaram um drone pra entregar material radioativo em um prédio do governo japonês. Em abril de 2015, um drone com vestígios de material radioativo pousou no telhado do gabinete do primeiro-ministro Shinzo Abe. De acordo com a agência de notícias Kyodo, o objetivo do atentado que felizmente não causou vítimas, seria o de protestar contra a política de energia nuclear do país.

Veículos aéreos não tripulados também podem ser empregados até como vetores para ataques cibernéticos. Atualmente, dispositivos sem fio são onipresentes em ambientes domésticos e de trabalho em todo o mundo e se um atacante habilidoso é capaz de obter proximidade física do seu alvo, tais alvos se tornam mais vulneráveis à invasões ou a interceptação de seu tráfego de informações. Wi-Fi, Bluetooth e tecnologia celular são meios que as pessoas empregam todos os dias, mas que emitem sinais que podem ser interceptados. Por meio desse vazamento de informações, pessoas podem ser rastreadas, redes podem ser mapeadas e dispositivos vulneráveis podem ser hackeados. As capacidades crescentes e o barateamento dos custos dos drones comerciais contribuem para torná-los uma plataforma muito útil para alguns tipos de cyber-ataques. Enquanto a segurança das instituições está firmemente baseada em cercas, muros, fossos, grades, concertinas e portões para impedir o acesso físico não autorizado a edifícios, fica difícil dissuadir ações desses atacantes não-convencionais. Usando drones especialmente equipados, hackers podem invadir redes Wi-Fi institucionais ou corporativas. Com um drone, certas barreiras de segurança física são facilmente contornáveis e a segurança fica irremediavelmente comprometida. Ressalte-se que muitas autoridades possuem o hábito de trabalhar em suas residências com seus computadores pessoais portáteis, os quais, muitas vezes, não contam com recursos de segurança robustos e eficazes, como aqueles que são encontrados nos órgãos executivos governamentais e em suas redes computacionais. A Secretária de Estado norte-americana Hillary Clinton usava provedores de e-mail comerciais para tratar de assuntos de serviço... A regra é clara: sempre será mais fácil atingir alvos em locais menos protegidos! Para um adversário com conhecimento técnico, os drones podem se constituir na solução ideal para superar obstáculos físicos enquanto que o espectro de radiofrequência é um ambiente de ataque que sempre poderá ser explorado com grande efeito.





Drone comercial adaptado para cyberataques.

A capacidade dos drones como vetores de artefatos explosivos é igualmente algo temível. Hoje não mais se desdenha a possibilidade de criar verdadeiros I.E.D aéreos, conduzidos para detonar precisamente, onde seus danos possam ser maximizados e o risco do emprego de drones pelo terrorismo é real.

Em fevereiro de 2015, pequenas aeronaves multi-rotores não identificadas foram avistadas em Paris nas imediações da Praça da Concórdia, na área dos Inválidos e ao longo do rio Sena. Em março do mesmo ano, três jornalistas da Al-Jazeera foram presos, após empregar drones no espaço aéreo da capital francesa, que é proibido para tais aparelhos. Não se descartou, à época, que pudesse se tratar de um ensaio pra a execução de múltiplos atentados terroristas na cidade. Nos EUA, drones operados por desconhecidos já tinham sido abatidos ao sobrevoar a Casa

Branca. Na abertura dos Jogos Olímpicos no Rio de Janeiro, cerca de meia dúzia de aparelhos remotamente controlados tiveram de ser neutralizados pelas contramedidas eletrônicas da segurança. Ainda que todos tivessem uma carga útil de câmeras filmadoras, desses, pelo menos um tinha capacidade de transportar uma carga útil da ordem de 2kg. Não precisa muita imaginação para antever o que uma carga explosiva desse peso pode fazer numa multidão ou se dirigida contra uma refinaria, oleoduto ou indústria química!

Em 4 de agosto de 2018, o Ditador Venezuelano Nicolás Maduro teria sido alvo de um atentado com drones pequenos transportando explosivos, quando assistia a uma parada numa das principais avenidas de Caracas. Toda a ação de ataque e a reação da segurança presidencial, de tão caricatural, deixou muitos com a impressão de que se tratou de uma ocorrência inabilmente encenada pelo próprio governo venezuelano.

O Hezbollah tem usado drones desde 2004, uns transportando câmeras, enquanto que outros transportando explosivos. O Grupo Hezbollah afirma que seus drones Mirsad são construídos localmente, eles parecem ser versões modificadas (ou exportadas clandestinamente) do drone iraniano de vigilância Mohajer. O Mirsad é um pequeno avião com motor a pistão, envergadura de 3m e tem sido um alvo relativamente fácil para os sistemas de defesa aérea israelenses.

Os conflitos no Iraque e na Síria viram a ascensão de uma nova forma de guerra não tripulada, o uso em larga escala de drones armados de fácil aquisição. Enfrentando dificuldades para manter sua guerra convencional, o Estado Islâmico aderiu a novos e não-tradicionais métodos de ataque – incluindo o emprego de drones para reconhecimento de terreno e para bombardear seus inimigos. Os militantes do grupo Estado Islâmico conseguiram amealhar uma significativa frota de micro UAV, mantida graça às aquisições numerosas efetuadas por empresas de fachada no Reino Unido, Bangladesh e Espanha, bem como por consumidores com identidades falsas. Em grande parte, graças ao esforço dos irmãos Sujan e Ataul Haque Sobuj (empreendedores na área de TI em Bangladesh, onde fundaram uma filial local do Estado Islâmico e começaram a transformar seu império tecnológico na rede de abastecimento da frota de drones do E.I.), as empresas encomendam os drones e os remetem para os vários afiliados do Estado Islâmico ao redor do mundo. Os irmãos usavam suas empresas para comprar drones e peças de drones de nove fabricantes diferentes do Canadá ou dos Estados Unidos. Quando podiam, faziam as transações via PayPal e usavam nomes ocidentais falsos. Sujan e seu irmão empregavam diferentes empresas e diferentes pseudônimos para comprar outras peças para os drones – como câmeras, GPS e antenas para aumentar o alcance do controle do piloto. Os drones empregados são os típicos quadricópteros, de prateleira, que são comprados em outros países e então enviados para as fronteiras do Estado Islâmico e modificados em fábricas dissimuladas, de fundo de quintal, antes de estarem aptos para serem usados no campo de batalha. O esforço do Estado Islâmico por drones foi alimentado por equipamentos baratos, ao alcance dos consumidores, disponíveis desde o lançamento do DJI Phantom em 2013. Este quadricóptero voa a pouco mais de 30 km/h com autonomia de 20 minutos, enviando de volta vídeos em alta resolução a uma distância de 1,6 km, e chega nas mãos do E.I. por menos de US$ 2.000,00. Um rastreamento, efetuado a partir de drones abatidos e acidentados, ajuda a compreender a amplitude e a complexidade dessa rede de abastecimento do grupo: um drone foi adquirido num site indiano em agosto de 2016, ativado na Inglaterra em

novembro do mesmo ano, e recuperado num campo de guerra no Iraque pouco tempo depois!

No início de 2016, drones de asa fixa do Estado Islâmico já realizaram ataques no estilo kamikaze no Iraque e na Síria. Estes foram substituídos por quadricópteros, reutilizáveis, lançando granadas, que se tornaram cada vez mais comuns. Os quadricópteros são difíceis de derrubar com armas de fogo. O Estado Islâmico começou a usar drones para filmar ataques suicidas em vídeos de propaganda para recrutamento e depois aperfeiçoou o uso dessas máquinas baratas em combate. Em Mosul drones localizaram alvos, ajudaram a ajustar a pontaria dos morteiros e ainda atingiram seus alvos com granadas. O Estado Islâmico demonstrou a capacidade de empregar pequenos drones comerciais para transportar cargas explosivas, sendo que, também adaptaram as aeronaves para lançar, com precisão pequenas bombas feitas com ogivas de granadas de 40mm adaptadas a aletas. O mecanismo de armar habitual das granadas foi substituído por um anel que é automaticamente retirado quando a munição é libertada. A ogiva tem um raio letal de 5 m e pode penetrar chapas de aço de 50 mm. A ideia dos pequenos drones de bombardeiro, tão bem sucedida, foi até copiada pelas forças de segurança do Iraque que hoje os empregam em missões de contra terror. O drone Phantom se constituiu num sucesso comercial, e gerações cada vez mais capazes vem surgindo a seguir, bem como muitos imitadores. O Exército iraquiano, alvo constante do ataque dos pequenos quadricópteros, passou a empregar os mesmos recursos, surpreendendo os insurgentes e os fazendo experimentas um pouco de seu próprio veneno.

Hoje, o Estado Islâmico não foi completamente derrotado; e ainda que esteja longe do poderio crescente do Califado de 2015, tropas do grupo terrorista e afiliados ainda são uma presença mortal no Iraque, na Síria, na África e no Afeganistão.

Em 14 de setembro de 2019, duas das maiores instalações petrolíferas da Arábia saudita foram atacadas e entraram em chamas, ameaçando a produção de combustível do país. Os rebeldes Houtis, do Iêmen, assumiram a autoria do atentado, que, afirmam, ter sido executado com drones de diversos modelos e dimensões, capazes de transportar cargas de úteis de até 45kg cada.

COMO OS DRONES SÃO CONTROLADOS

As aeronaves remotamente pilotadas são controladas por diferentes métodos. O Controle por Bluetooth é normalmente usado em drones de alcance muito curto (até 20 m) e com um pouquíssima autonomia de voo, que normalmente são classificados como "brinquedos". Os Controles por Wi-Fi também são de curto alcance e com autonomia de voo limitado, também são classificados como "brinquedos".

A grande maioria dos drones comerciais e muitos dos modelos de uso militar empregam Controle por Rádio (RF). Normalmente tais drones operam em várias frequências (900 MHz, 1,3 GHz, 2,4 GHz e 5,8 GHz), sendo que a maioria dos veículos aéreos não-tripulados disponíveis comercialmente opera nas faixas de 2,4 GHz e 5,8 GHz. Alguns veículos usam ambas as faixas ao mesmo tempo para permitir o controle de voo e a transmissão de vídeo ao vivo. O alcance de recepção depende de vários fatores como a potência do transmissor, interferência / obstáculos, etc. Nos drones recreativos de tamanho menor é de aproximadamente 2 km; No entanto, com a antena e os receptores certos, potência suficiente e interferência mínima, pode chegar até 70km.

Os sistemas de telefonia celular 3G e 4G também são empregados para controlar drones e permitem fazê-lo por longo alcance e geralmente com comunicações via Internet. O alcance máximo é limitado apenas pela capacidade de

energia da bateria (no caso dos motores elétricos) ou combustível alocado para o voo e pela qualidade do sinal da operadora móvel disponível.

Aeronaves não-tripuladas também podem ser controladas a partir de satélites, conjugando o longo alcance de voo com a possibilidade de dispor os controladores a distâncias intercontinentais. Há também modelos que possuem controles autônomos, conjugados a GPS. Nesse caso o operador do drone estabelece um plano de voo que é executado pela aeronave via GPS. Em ambos os modos de operação, o alcance máximo de voo só é limitado apenas pela resistência do drone.

Ainda há sofisticados sistemas em que a aeronave opera de forma autônoma, seguindo um plano de voo que acompanha os contornos do terreno, referenciando acidentes geográficos e estruturas acima do solo. Esse modo de operação é empregado nos sofisticados aparelhos autônomos de reconhecimento.

MÉTODOS DE DETECÇÃO

Há uma grande quantidade de métodos para detecção de drones: Detecção visual ou auditiva, detecção instrumentada de áudio (através de microfones sensíveis), por Imagem térmica, por radar, por rádio (RF) e Wi-Fi. A detecção de um drone pequeno e ágil, a baixa altitude é uma capacidade importantíssima, sobretudo para a manutenção da segurança de dignitários nos dias de hoje.

A esmagadora maioria dos drones pequenos são propelidos por motores elétricos, os quais são bem mais silenciosos do que os motores a gasolina empregados por aeromodelos. Operando em locais abertos, por vezes o ruído de tais motores elétricos será completamente abafado pelo ruído do ambiente, o que vai permitir uma aproximação segura de um eventual drone atacante, até que ele esteja perigosamente perto do alvo. Equipamentos como microfones direcionais sensíveis podem ser usados para a vigilância anti-drones, conjugados a bancos de dados com as assinaturas acústicas de drones conhecidas; contudo muitos veículos podem ser personalizados, com hélices e motores customizados, que modificariam sua assinatura de áudio, dificultando assim a detecção.

A detecção visual com binóculos é difícil, até pelo fato de que as pequenas aeronaves podem receber uma pintura capaz de camufla-las contra o céu ou contra acidentes do terreno. Numa detecção instrumentada, uma câmera com zoom e inteligência embarcada localiza o objeto aéreo em movimento e tenta diferenciar entre um drone pequeno e pássaros, com base no tamanho, trajetória de voo e estilo de movimento. Uma variação da detecção com câmeras emprega câmeras térmicas que buscam a identificação da assinatura de calor de um drone. Não se trata de uma tarefa fácil pois a maioria dos UAVs minis e pequenos é construído em plástico, e operando com motores elétricos irradiam uma assinatura de calor extremamente pequena.

A detecção de Rádio envolve o monitoramento das frequências de 2,4 GHz e 5,8 GHz para transmissões de drones. No caso do Wi-Fi, a detecção é permitida porque muitos drones comerciais de baixo custo têm SSIDs (Sigla para Service Set Identifier (“Identificador do Conjunto de Serviços”, em português, ou comumente, “nome de rede”) identificáveis e endereços MAC (um endereço de controle de acesso à mídia de um dispositivo, um identificador único atribuído a uma interface de rede) que são transmitidos.

A Detecção por radar só é possível contra aparelhos de maiores dimensões. Em face de drones pequenos, a detecção não é possível usando sistemas de radar de

detecção de aeronaves padrão. Apenas um aparelho de cobertura contínua de 360 graus especializado é capaz de identificar objetos muito pequenos e lentos, como drones, e necessita do uso de técnicas avançadas de processamento de sinal para diferenciar entre pássaros e os UAVs

CONTRAMEDIDAS

Existem muitos métodos documentados para desativar, interromper ou sequestrar drones, compreendendo desde ataques físicos ao emprego de recursos digitais.

Métodos Balísticos - Desativação de um aeronave remotamente pilotada empregando um projétil, por exemplo Pistola de paintball, espingarda, catapulta e armas de rede. Munições explosivas podem se constituir num problema na medida que, não impactando o alvo ou não conseguindo explodir em suas proximidades, tais projéteis podem cair e gerar danos colaterais indesejados.

Emprego de Lasers – Atualmente, lasers de alta potência conjugados a sistemas de rastreamento automático de radar e câmeras de pontaria vem sendo apresentados como a melhor opção para derrubar drones, literalmente derretendo seus componentes.

Jamming - Vários métodos estão disponíveis para controlar as instruções direcionais ou os dados de posição recebidos pelos drones. A maioria dos dispositivos de interferência de uso civil, portáteis, tem um alcance limitado (cerca de 50m), no entanto, o equipamento militar é capaz de bloquear grandes áreas de RF, 3G / 4G, Wi-Fi e GPS.

Armas de micro-ondas - Produzem um feixe de energia focalizado projetado para interromper as comunicações com a fonte controladora ou mesmo para destruir componentes internos sensíveis.

Uso de animais - Os drones de até 7kg têm sido alvos fáceis para aves de rapina especialmente treinadas.

Drones Caçadores - UAVs especialmente projetados que interferem nas comunicações Wi-Fi, carregam e lançam redes ou usam táticas kamikaze para desabilitar outros UAVs, explodindo-os ou colidindo com eles.

Jatos de água – Diversos corpos de bombeiros dos EUA já empregaram com sucesso os jatos de alta pressão contra drones que sobrevoavam áreas de incidente de forma não autorizada.

Sequestro de Frequências - O *Hijacking* do sinal de Wi-Fi provou ser um sucesso por meio do uso de ataques de desautenticação que interrompem as comunicações entre o drone e o controlador e estabelecem uma nova conexão com o *sequestrador*. Muitos dos UAVs de "brinquedo", de baixo custo, não têm segurança na conexão Wi-Fi e, consequentemente, qualquer terceiro pode se conectar ao aparelho e passar a controla-lo. SkyJack é um programa que detecta e desativa qualquer cliente conectado ao drone e o bypassa.

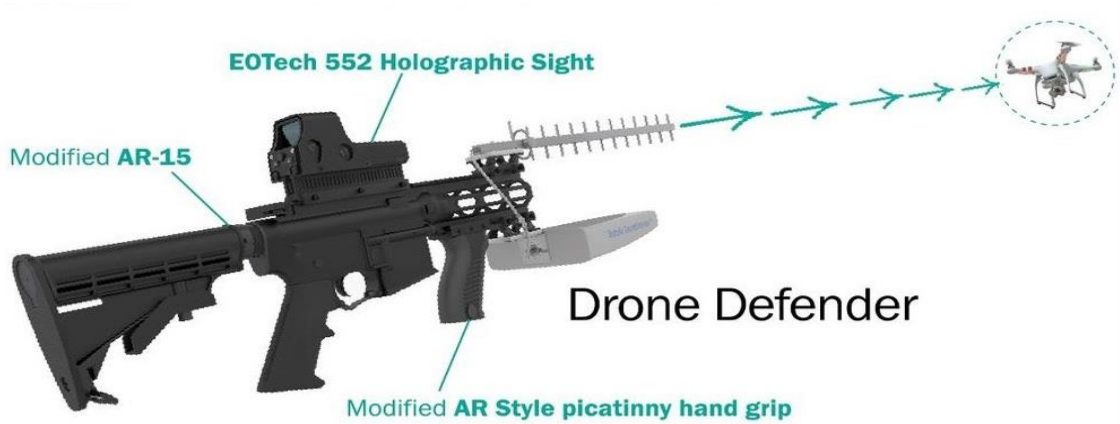
Spoofing - técnicas de falsificação de RF ou GPS podem ser usadas para retransmitir informações falsas para um drone. Em dezembro de 2011, o Irã alegou ter capturado uma aeronave remotamente pilotada dos Estados Unidos interrompendo as comunicações por satélite e transmitindo dados de GPS falsos para fazer o UAV

pousar no Irã. Estudando modelos de drones comerciais, é possível projetar programas que percorram as frequências de comunicação até encontrar as transmissões de equipamentos específicos, A partir desse ponto, tais programas seriam capaz de extrair a ID do dispositivo e interferir maliciosamente nos comandos da aeronave.

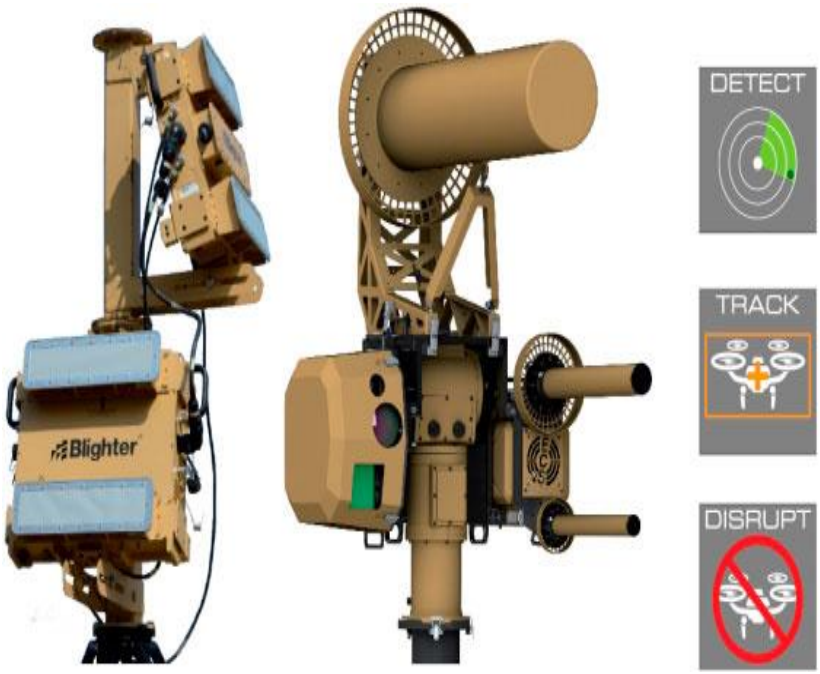
Ataques baseados em nuvem - Um conjunto de softwares de controle baseados em nuvem estão amplamente disponíbilizados, permitindo que empresas comerciais de drones gerenciem frotas de UAVs. É possível que a tecnologia baseada em nuvem seja vulnerável a ataques que permitiriam a uma pessoa mal-intencionada assumir o controle dessas frotas de aeronaves.

Ataques baseados no cliente - O software fornecido pelos fabricantes de drones raramente tem segurança reforçada e já está provado que, por meio da engenharia reversa, as vulnerabilidades dos aplicativos empregados nas comunicações com essas aeronaves podem ser encontradas e empregadas para utilizar os aparelhos de forma criminosa.

No Brasil, em dezembro de 2015, o Departamento de Controle do Espaço Aéreo (DECEA), publicou uma regulamentação para os drones, exigindo que, para emprego em áreas povoadas ou especificamente sobre concentrações de pessoas em eventos, se solicite previamente autorização expressa ao próprio DECEA. Essa providência faz sentido, e é de se esperar que seja expandida, para cobrir por exemplo situações de emergências ou desastres naturais, em que drones empregados por canais de TV e agências de notícias para colher imagens possam por em perigo o trabalho dos helicópteros de resgate, bombeiros ou policiais. O potencial uso de drones, dos mais diversos tamanhos, em toda sorte de atos ilegais criou uma dor de cabeça a mais para a segurança, provocando uma demanda por equipamentos de contramedidas eletrônicas anti-drones, com soluções que vão desde a equipamentos portáteis semelhantes a fuzis (que emitem um feixe de interferência que impeça o controle de pequenos drones comerciais, levando-os a cair) até estações complexas, com numerosas antenas e conjugadas a radares ou câmeras de vídeo infravermelhas, capazes de promover uma cobertura diuturna de maior alcance e eficácia.



Tais sistemas altamente sofisticados e dispendiosos como o AUDS (Anti-UAV Defense System), de fabricação britânica, combinam detecção por radar (radar de vigilância Dopller operando na banda Ku), acompanhamento e classificação eletro-ópticos (uma câmera colorida de alta resolução e outra IV) e capacidade de inibição por emissões de radiofrequência (através do inibidor RF que seletivamente interfere nos canais de comando e controle da ARP), se dedicam a desabilitar aeronaves remotamente tripuladas que estejam sendo usadas em áreas remotas ou urbanas para ataques terroristas, espionagem ou atividades ilegais contra infraestruturas críticas. O AUDS alcance de detecção é de 8km, a seção radar mínima do alvo é 0,01m2, com cobertura de 180° em azimute e 4W de potência.



AUDS (*Blighter Surveillance Systems).*

No Brasil, segmentos da mídia chegaram a estranhar que se gastasse com equipamentos de contramedidas anti-drone, para a proteção de prédios públicos em Brasília. Tendo um Presidente da República que já foi alvo de um atentado e com todos os riscos que pesam sobre ele, não se poderá descartar a hipótese de que o mesmo pudesse vir a ser vitimado por um pequeno Kamikaze explosivo guiado a distância...

Um recurso para viabilizar uma última linha de defesa para derrubada de drones multirotores de pequenas dimensões é o uso de munições especiais em espingardas calibre 12, as quais são normalmente empregadas em seguranças de dignitários ao redor do mundo.

A munição SKYNET possui um projétil se fragmenta a poucos metros da boca do cano da arma, em partes que continuam unidas por um resistente fio de kevlar. À medida que essas partes se separam e se estendem para fora, é criada uma teia com 1,5m de diâmetro. Essa munição age como uma daquelas boleadores de vaqueiro. Quando a munição atinge o drone, as amarras e as peças redondas envolvem o drone, interferindo nas hélices e forçando o drone ao solo. Se a munição errar o alvo, ela será projetada para cair de paraquedas com segurança no solo para reduzir qualquer dano ou lesão indesejada. Nos Estados Unidos essa munição é comercializada em pacotes com três cartuchos.

A tecnologia dos veículos aéreos não tripulados chegou para ficar, e o emprego, sobretudo das aeronaves de pequenas dimensões, é algo que vai exigir constante preocupação das equipes voltadas para a proteção de autoridades, tanto em seus locais de base quando em seus deslocamentos. Lembremo-nos sempre da máxima de que, onde quer que você possa ser esperado, lá o perigo poderá estar te espreitando!