Análise do Estado da Arte em Segurança Cibernética com Drones

Pedro Henrique Ulrich[1], **Jeferson Campos Nobre**[1]

[1]Universidade do Vale do Rio dos Sinos (UNISINOS)
Av. Unisinos – 950 – Cristo Rei – São Leopoldo – RS – Brazil

pedrohulrich@hotmail.com, jcnobre@unisinos.br

Abstract. *The use of drones is expanding rapidly as new applications are created for these devices. As this expansion occurs, Cybersecurity issues arise which need to be addressed for greater control of your operation. This article reviews the literature on cybernetic security with drones, focusing on the analysis of real and simulated attacks. In the course of this review, it is proposed to perform an analysis of the command, control and communication forms of the drones. Besides that, the attacks performed on drones are analyzed based on the principles of Information Security, that is, the attacks are divided into Confidentiality, Integrity and Availability (CIA). From this analysis, the possible research directions on Cybersecurity with drones are presented.*

Resumo. *A utilização de drones está se expandindo rapidamente conforme novas aplicações são criadas para estes dispositivos. Conforme essa expansão ocorre, surgem problemas de Segurança Cibernética que precisam ser abordados para um maior controle de sua operação. Este artigo realiza uma revisão da literatura sobre segurança cibernética com drones, concentrando-se na análise de ataques reais e simulados. No decorrer desta revisão, propõe-se a realização de uma análise das formas de comando, controle e comunicação dos drones. Além disso, os ataques realizados em drones são analisados com base nos princípios da Segurança da Informação, ou seja, os ataques são divididos em Confidencialidade, Integridade e Disponibilidade (CID). A partir desta análise são apresentadas as possíveis direções de pesquisa em Segurança Cibernética com drones.*

1. Introdução

A aviação apresenta muitas ameaças de segurança e privacidade. Em um passado não muito distante, apenas pilotos treinados e certificados recebiam autorização para pilotar aeronaves [Altawy and Youssef 2016]. Hoje, qualquer pessoa pode operar uma máquina voadora, podendo gerar interferência nos sistemas de aviação e sobrevoar pessoas com câmeras e microfones. Os veículos aéreos não tripulados (VANTs), mais popularmente conhecidos como drones, estão sendo usados em operações civis e militares, entrega de produtos, agricultura, pesquisa, mapeamento, inspeção de infraestruturas críticas de distribuição de energia e vigilância. Segundo um relatório da [Gartner 2017], até 2020, 3 milhões de drones comerciais e pessoais devem ser vendidos por ano, o que deve gerar um faturamento de cerca de 11,2 bilhões de dólares por ano.

O controle de um drone é realizado através de uma interface (controle remoto, computador, simulador, etc.), já que os pilotos não ficam a bordo. Os elementos físicos a

bordo de um drone empregam uma rede de sensores e atuadores que se comunicam com o sistema de controle de solo por meio de um enlace sem fio. Dessa forma, muitas vezes o sistema de drones pode ser suscetível a ataques que visam os elementos cibernéticos ou físicos, a interface entre eles, o enlace sem fio ou mesmo uma combinação de múltiplos componentes [Constantinides and Parkinson 2008].

Um exemplo da segurança em drones foi descrito por [Hartmann and Steup 2013], onde um drone militar foi tomado por uma parte não autorizada. Este caso ocorreu quando uma unidade iraniana de guerra cibernética conseguiu pousar um drone norte-americano que violou seu espaço aéreo. Embora o cenário exato não seja confirmado, os eventos indicam que foi aplicado uma combinação de ataques cibernéticos, onde inicialmente todas as comunicações legítimas com o drone foram interrompidas. Um ataque de GPS spoofing foi lançado para alimentar o drone com dados modificados e para fazê-lo pousar no Irã, enganando o drone como se ele estivesse pousando em sua base [Humphreys 2012].

Alguns trabalhos foram desenvolvidos analisando os principais aspectos em segurança com drones. [Altawy and Youssef 2016] realizaram um *survey* sobre ameaças físicas e cibernéticas dos drones, onde elencaram os ataques com base nos principais componentes do drone. [Krishna and Murphy 2017] examinaram a literatura científica e comercial sobre segurança cibernética para drones, concentrando-se em ataques reais e simulados. No entanto, nenhum trabalho realizou esta análise com base nos três princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

O presente artigo apresenta uma revisão da literatura sobre segurança cibernética com drones. Experiências e publicações científicas foram analisadas com o propósito de verificar vulnerabilidades e ameaças presentes em possíveis ataques ao sistema de drones. A revisão inclui ataques em drones de qualquer tamanho, pois determinados ataques podem ser realizados tanto em drones grandes como em drones pequenos.

Este artigo está estruturado da seguinte maneira. Na Seção 2, descreve-se os conceitos iniciais, as formas de comando, controle e comunicação e análise de segurança em drones. Na Seção 3, é descrito os trabalhos relacionados com este artigo. A Seção 4 tem como objetivo descrever as possíveis direções de pesquisa e por fim, na Seção 5, são apresentadas as conclusões deste trabalho.

2. Aspectos Teóricos Sobre Drones

Segundo o [DECEA 2015], o termo drone (em português: zangão, zumbido) é apenas um nome genérico e informal, originado nos Estados Unidos e que vem se difundindo mundo a fora, para caracterizar todo e qualquer objeto voador não tripulado, seja ele de qualquer propósito (profissional, recreativo, militar, comercial, etc.), origem ou característica. A seguir é apresentado os conceitos iniciais, suas formas de comando, controle e comunicação e a segurança em drones.

2.1. Conceitos Iniciais

De acordo com [Marshall et al. 2011], no final de 1916, com a guerra em curso na Europa, a Marinha dos EUA financiou Elmer Sperry para começar a desenvolver um torpedo aéreo não tripulado. O intuito inicial era que fosse construído um avião pequeno, leve, que pudesse ser lançado sem um piloto e ir sozinho até o inimigo, explodindo junto com ele. O projeto resistiu a uma série de contratempos, acidentes e falhas de diversas peças que

formavam o Torpedo Aéreo Curtis N-9 [Marshall et al. 2011]. A equipe de Elmer Sperry perseverou e finalmente no dia 6 de março de 1918 o protótipo Curtis não tripulado foi lançado com sucesso, surgindo assim o primeiro "drone" verdadeiro do mundo.

Diversos termos são utilizados para definir drones. Em inglês *Unmanned Aerial Vehicle (UAV)*, já em português pode ser denominado como Veículo Aéreo Não Tripulado (VANT). O Regulamento Brasileiro da Aviação Civil Especial nº 94 (RBAC-E nº 94) da Agência Nacional de Aviação Civil (ANAC) para drones no Brasil utiliza os termos Aeromodelo e Aeronave Remotamente Pilotada, os Aeromodelos são usados para fins recreativos e as Aeronaves Remotamente Pilotadas (*Remotely-Piloted Aircraft – RPA*) são utilizadas para fins comerciais, institucionais ou experimentais [ANAC 2017].

Os drones variam drasticamente de tamanho, alguns são tão pequenos que podem caber na palma da mão e outros são tão grandes quanto aeronaves tripuladas. A ANAC categorizou os drones de uso comercial, institucional ou experimental (RPA) em três classes: classe 1, classe 2 e classe 3.

- Classe 1: RPA com peso máximo de decolagem maior que 150 kg.
- Classe 2: RPA com peso máximo de decolagem maior que 25 kg e menor ou igual a 150 kg.
- Classe 3: RPA com peso máximo de decolagem menor ou igual a 25 kg.

Atualmente, as operações de drones no Brasil devem seguir as regras da ANAC, que são complementadas com as normas estabelecidas pelo Departamento de Controle do Espaço Aéreo (DECEA) e pela Agência Nacional de Telecomunicações (ANATEL). De acordo com o [DECEA 2015], a ANAC trata de assuntos técnicos/operacionais voltados às condições das aeronaves e situação dos pilotos, a ANATEL realiza a homologação de drones que possuem transmissores de radiofrequência e o DECEA trata do acesso ao espaço aéreo.

2.2. Comando, Controle e Comunicação

O controle das ações de um drone são realizadas conforme o grau de autonomia do equipamento. Segundo [Altawy and Youssef 2016], os drones podem ser totalmente controlados remotamente por um operador através de uma Estação de Controle Terrestre (*Ground Control Station - GCS*), que pode ser um tablet, controle remoto, computador, entre outros. Também podem ser totalmente autônomos, ou seja, podem voar sem a intervenção do operador da decolagem ao pouso e dependem de seus sensores para executar um conjunto de tarefas pré-programadas. Dentro deste contexto e dependendo do grau de domínio exercido por um operador humano, o controle de um drone foi dividido por [Altawy and Youssef 2016] em três categorias:

- Controle remoto do piloto: este tipo de controle é conhecido como automação estática do operador, onde o sistema de controle é projetado de modo que todas as decisões sejam tomadas por um operador humano.
- Controle remoto supervisionado: este tipo de controle é comumente conhecido como automação adaptável. Ele permite que o drone realize seu voo independentemente dos comandos humanos e também possibilita a intervenção humana ao mesmo tempo.

- Controle autônomo completo: esta categoria de controle é conhecida como automação estática do sistema, na qual o drone realiza todas as decisões necessárias para a conclusão do voo.

A arquitetura do sistema de drones é formada por três elementos principais, que são o drone, a GCS e o enlace de comunicação de dados. Conforme [Marshall et al. 2011], outros elementos também podem compor sua arquitetura, como, por exemplo, o elemento humano e a carga útil a ser transportada. Além destes elementos, o drone pode ser composto por uma estrutura com sistema de propulsão, controlador de voo, um sistema de navegação de precisão e um sistema de detecção e controle. A Figura 1 apresentada a seguir ilustra a arquitetura de alto nível de um sistema de drones e seus elementos principais.

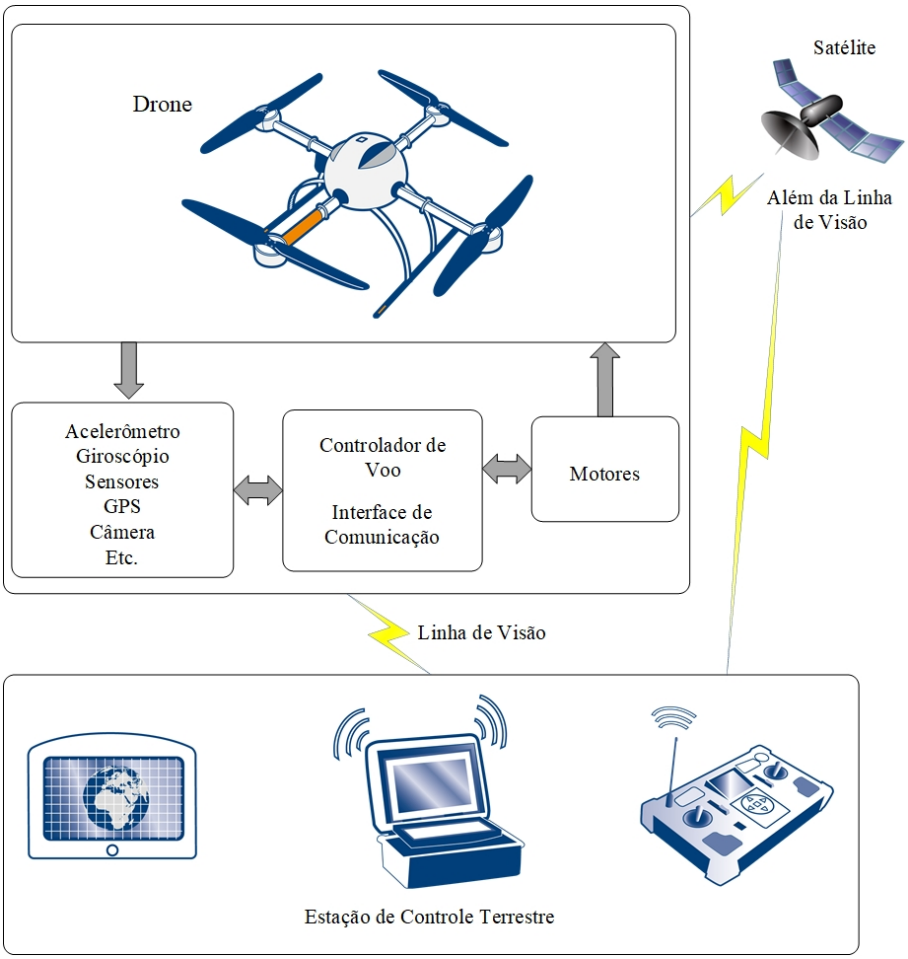

Figura 1. Arquitetura de alto nível de um sistema de Drones. Adaptado de [Altawy and Youssef 2016].

A presente pesquisa se foca nos componentes principais para a análise. Sendo assim, considera-se que o drone contém um controlador de voo e um conjunto de sensores. Em seguida, apresenta-se uma visão geral dos elementos principais da arquitetura do sistema de drones:

- Controlador de voo: é a unidade central de processamento do drone. De acordo com [Ebeid et al. 2017], ele controla os motores, interage com sensores internos

ou externos, navega e se comunica com a GCS. Os comandos da GCS são processados pelo controlador de voo e o mesmo envia as instruções para os atuadores, que são pequenos mecanismos que criam movimento de alguma parte do veículo.

- Sensor: o controlador de voo pode ter vários sensores integrados a bordo ou se comunicar com uma unidade de sensor externa. Os drones utilizam sensores para detectar alterações nas suas proximidades e para realizar manobras melhores. Os sensores do sistema de drones podem incluir acelerômetro, giroscópio, sensor de orientação magnética, módulo GPS e câmera eletro-óptica ou infravermelha [Altawy and Youssef 2016].
- GCS: é um centro de controle terrestre que fornece recursos para que os operadores humanos controlem e/ou monitorem os drones durante suas operações. Segundo [Marshall et al. 2011], as GCSs variam em tamanho físico, podendo ser pequenas como um transmissor de mão ou tão grandes quanto uma instalação autônoma com várias estações de trabalho. A GCS se comunica com o drone através de um enlace sem fio para enviar comandos e receber dados em tempo real.
- Enlace de comunicação de dados: refere-se ao enlace sem fio usado para transportar informações de conexão e controle entre o drone e a GCS. O sistema de comunicação do drone utiliza sinais de rádio e Wi-Fi para se comunicar com a GCS ou até mesmo com os outros drones. Conforme [Marshall et al. 2011], as operações dos drones podem ser divididas em duas categorias: linha de visão, onde os sinais de controle podem ser enviados e recebidos via ondas de rádio diretas e a outra categoria é além da linha de visão, onde o drone pode ser controlado por meio de comunicações via satélite ou por uma aeronave de retransmissão que também pode ser um drone.

2.3. Segurança em Drones

O aumento no uso de drones também acarreta um aumento em questões de segurança cibernética. Segundo [Altawy and Youssef 2016], a maioria dos padrões de aviação estabelecidos pelos órgãos reguladores ainda não cobre as ameaças cibernéticas associadas a integração dos drones.

A regulamentação RBAC-E nº 94 da ANAC e as regras do DECEA e da ANATEL são voltadas ao controle de peso máximo de decolagem, cadastro dos drones, restrição de voo em áreas sensíveis, operação somente em áreas distantes de terceiros e não possuem uma seção sobre segurança da informação [ANAC 2017]. Com base no cenário atual, pode-se verificar que a maioria dos usuários de drones não está ciente sobre os problemas de segurança e privacidade, onde enxergam apenas o lado recreativo destes dispositivos.

A análise de ameaças é um aspecto importante para garantir a segurança de um sistema, pois através delas pode-se descobrir vulnerabilidades no sistema de drones. Os ataques foram analisados levando em consideração os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade (CID).

2.3.1. Confidencialidade

Este pilar tem como objetivo ter a informação disponível somente para pessoas autorizadas. Segundo [Javaid et al. 2012], uma das maneiras mais comuns de comprometer a

segurança desta propriedade é a interceptação de informações e as principais ameaças são baseadas em software, vírus, malwares, trojans, etc.

O ataque de GPS spoofing é comumente executado em drones [Vattapparamban et al. 2016]. A navegação dos drones pode depender dos sinais de GPS recebidos e processados pelo receptor de GPS a bordo. Normalmente as transmissões por GPS são de livre acesso, visto que não utilizam criptografia e mecanismos de autenticação. De acordo com [Vattapparamban et al. 2016], a ideia do GPS spoofing é transmitir coordenadas de GPS falsas para o controlador de voo do drone, sendo assim, poderá sequestrar o drone e posteriormente assumir o controle total do equipamento. Para ocorrer um ataque de GPS spoofing, um transmissor é utilizado para enviar sinais falsos de GPS, forçando a vítima a sincronizar com os sinais do atacante.

O controlador de voo e a GCS estão vulneráveis a ataques que utilizam softwares maliciosos. Um exemplo de *malware* que infecta os drones é um software conhecido como *Maldrone*, que após instalado no drone permite que o atacante assuma o controle do equipamento. Segundo [Dey et al. 2018], o *Maldrone* atua como um *proxy* para o controlador de voo e as comunicações do sensor do drone, permitindo assim a injeção dos valores desejados para ambas as comunicações.

As informações trocadas entre o drone e a GCS incluem os feeds de telemetria e os comandos emitidos pela GCS. Um ataque de interceptação de feed de vídeo foi executado em drones Predator, que resultou em consequências desconhecidas. Conforme [Krishna and Murphy 2017], este ataque foi realizado pelo Irã em drones norte-americanos em dezembro de 2009 e foi identificado quando militares americanos no Iraque encontraram o vídeo interceptado em um *laptop* apreendido de um militante. Ainda segundo [Krishna and Murphy 2017], os feeds de vídeo estavam com a criptografia desativada por questões de desempenho e foram interceptados usando o software *SkyGrabber*, que é utilizado para interceptar vídeo usando antena de satélite.

Os drones controlados por Wi-Fi usam os padrões IEEE 802.11. Toda a comunicação entre o drone e a GCS que utiliza a rede Wi-Fi pode ser vulnerável a violações de segurança. Para as comunicações sem fio, os dispositivos devem saber com quem se comunicam antes do início das sessões de comunicação. De acordo com [He et al. 2016], *frames* de gerenciamento são usados para estabelecer essa associação inicial e se estes *frames* não estiverem protegidos, os dispositivos sem fio estarão sujeitos a ataques de *Deauthentication*. O software *SkyJack* pode ser usado para detectar todas as redes sem fio e forçar a desautenticação dos operadores de seus drones, para posteriormente se autenticar como um novo operador e ter o drone sob seu controle [Vattapparamban et al. 2016].

2.3.2. Integridade

O pilar de integridade visa garantir que não houve alterações nas informações. Isso significa que o processo de transmissão de mensagens não é interrompido e as informações recebidas devem ser exatamente as mesmas que foram enviadas. Se não houver proteção de integridade, os ataques mal-intencionados ou a interferência de canal sem fio podem fazer com que as informações sejam modificadas ou até mesmo destruídas [He et al. 2016].

Os drones autônomos de baixa altitude podem contar com o vídeo capturado por

suas câmeras para navegação e prevenção de colisões. Conforme [Deligne 2012], normalmente o processo é iniciado pelo controlador de voo solicitando o vídeo capturado a partir do *kernel* do sistema operacional do computador controlador de voo, emitindo uma chamada de sistema. Um atacante que tenha conhecimento dos parâmetros do sistema e seja capaz obter acesso ao controlador de voo pode realizar um ataque de modificação, interceptando as chamadas do sistema emitidas para o *kernel* e substituindo a gravação genuína por uma modificada [Altawy and Youssef 2016]. Como consequência deste ataque, o drone pode ser aterrissado em um local diferente do originalmente planejado.

Um ataque de *replay* intercepta os dados em transmissão e os retransmite mais tarde. Segundo [He et al. 2017], a repetição de solicitações ARP (*Address Resolution Protocol*) pode ser usada para quebrar a chave de criptografia em uma comunicação Wi-Fi. Inicialmente o atacante intercepta uma solicitação ARP e, em seguida, começa a retransmitir o mesmo pacote ARP repetidamente. Os autores afirmam que cada vez que uma solicitação ARP repetida atinge o drone com o endereço IP especificado na solicitação, uma resposta ARP é retornada pelo drone e ao repetir um grande número de solicitações o atacante pode violar a chave de criptografia. Para implementar este ataque, o conjunto de ferramentas *Aircrack* também pode ser utilizado. Os ataques de *replay* interferem diretamente no pilar de integridade, porém também podem interferir na disponibilidade e na confidencialidade [Yagdereli et al. 2015].

2.3.3. Disponibilidade

O pilar de disponibilidade tem o objetivo de assegurar que os sistemas e serviços não fiquem indisponíveis para usuários autorizados. Conforme [Javaid et al. 2012], os ataques primários que podem afetar a disponibilidade são *Jamming* e *Denial of Service (DoS)*.

Um atacante que está tentando assumir o controle do drone pode realizar um ataque de *Jamming* desabilitando a recepção dos sinais de controle que são originados da GCS autêntica. Isto pode ser realizado com o envio de sinais interferentes de maior potência na mesma banda de frequência. De acordo com [Krishna and Murphy 2017], um ataque de GPS *Jamming* foi executado no drone S-100 Camcopter, resultando em uma colisão com o controle terrestre que feriu dois pilotos remotos e matou um engenheiro durante os testes.

O ataque de negação de serviço (*Denial of Service - DoS*) é caracterizado por uma tentativa de um invasor impedir que os usuários legítimos usem os recursos desejados. Baseiam-se principalmente no congestionamento ou no estouro da placa de rede do sistema, de modo que o sistema pareça estar indisponível. Segundo [Altawy and Youssef 2016], um ataque de DoS normalmente é lançado em drones pequenos, pois possuem processadores de potência moderada e inundar suas placas de rede com comandos aleatórios através do enlace de dados pode forçar esses drones a entrar em um estado inesperado e, possivelmente, interromper sua operação. A inundação da placa de rede é realizada com um ou mais tipos de pacotes de rede. Normalmente são utilizados os pacotes SYN, UDP, ICMP e Ping para este tipo de ataque [Javaid et al. 2012].

3. Trabalhos Relacionados

Esta seção tem o objetivo de apresentar alguns trabalhos relacionados que discutiram aspectos de segurança cibernética com drones. Os trabalhos relacionados utilizados como base para a revisão da literatura foram retirados de artigos científicos disponibilizados em portais na Internet, como, por exemplo, Association for Computing Machinery (ACM) e Institute of Electrical and Electronics Engineers (IEEE). O estudo procurou entender e levantar os diversos pontos entre os artigos, identificando conceitos iniciais, formas de comando, controle e comunicação e investigação sobre segurança em drones.

[Altawy and Youssef 2016] realizaram um *survey* sobre a análise dos principais aspectos de segurança e privacidade associados ao uso de drones, onde especificaram as ameaças com base nos principais componentes do drone. Os autores afirmam que a maioria dos ataques cibernéticos são contra diferentes componentes dos sistemas de drones e geralmente os ataques sofisticados que visam assumir o controle do drone combinam um ou mais ataques ao controlador de voo e ao enlace de dados.

[Krishna and Murphy 2017] examinaram a literatura científica e comercial sobre segurança cibernética para drones, concentrando-se em ataques reais e simulados. Os autores também dividiram os drones em grandes e pequenos, porém apenas listam as ameaças com o foco em mostrar o número de incidentes e estudos reportados, não acrescentando informações adicionais sobre a maioria das ameaças. Os autores comentam que o artigo concentra-se tanto em riscos conhecidos quanto em riscos teóricos para drones pequenos, embora a litetura inclua ataques em drone de qualquer tamanho, visto que esses riscos podem ser transferifos para os drones pequenos.

Não foram encontrados, no entanto, trabalhos que fazem esta mesma análise com base nos três princípios da segurança da informação: confidencialidade, integridade e disponibilidade. Atualmente, nenhum trabalho em português aborda questões de segurança cibernética relacionada aos drones. Em função dos trabalhos serem realizados em outros países, os mesmos também não consideram as regulamentações brasileiras em suas análises, como, por exemplo, a regulamentação RBAC-E nº 94 da ANAC para drones.

4. Possíveis Direções de Pesquisa

O objetivo desta seção é apontar possíveis direções de pesquisa com base na revisão da literatura realizada. Verificou-se que o campo da segurança cibernética para drones é relativamente novo, pois segundo [Altawy and Youssef 2016], a comunidade de segurança está apenas começando a identificar ameaças relacionadas aos drones e alguns assuntos ainda são pouco explorados. Sendo assim, em trabalhos futuros pretende-se realizar testes e simular ataques de drones.

Seria interessante um trabalho que abordasse um ataque sobre *De-authentication*, pois este ataque visa inicialmente desautenticar o operador do drone e posteriormente obter o controle do drone se autenticando como um novo operador. Este trabalho poderia utilizar um drone ou um simulador que permita a conexão dos usuários através dos protocolos 802.11. De acordo com [He et al. 2017], um ataque de *De-authentication* pode ser iniciado com a geração de uma série de *frames* que visam interromper a comunicação Wi-Fi com a GCS. Os autores também comentam que o conjunto de ferramentas *Aircrack* pode ser utilizado para implementar este ataque.

Outra possibilidade seria testar um ataque de DoS, visto que este é um dos ataques primários que pode afetar o pilar de disponibilidade. A comunicação sem fio é utilizada para controlar um drone e todos que estão ao alcance podem receber os sinais desta comunicação. Nesta comunicação, tanto o dispositivo de envio quanto o dispositivo receptor precisam utilizar o mesmo canal para se comunicar. Segundo [Rodday 2015], se o atacante conhece os canais utilizados (tecnologias padrões de comunicação ou frequências conhecidas para uso público), o mesmo poderia inundar estes canais com dados, impedindo que os sinais legítimos fossem recebidos pelo drone. Sendo assim, uma das alternativas seria encontrar uma forma de emular o canal de controle para aplicar um ataque de DoS.

Um ataque de *Man-in-the-Middle* também será verificado para tentar injetar comandos de controle e interagir com o drone. Conforme [Rodday 2015], duas coisas são necessárias para interferir no controlador de voo do drone, acesso ao canal de comunicação e ao *payload* correto. A primeira parte pode ser realizada usando a abordagem do DoS comentado anteriormente. Após o atacante é capaz de ouvir toda a comunicação trocada entre os dispositivos atacados, desta forma, o atacante pode inferir o *payload* e reconstruir comandos.

5. Conclusão

Este artigo realizou uma análise geral de ataques voltados ao sistema de drones. Durante a análise foram apresentados os principais elementos da arquitetura do sistema de drones. Além disso, os ataques cibernéticos foram classificados de acordo com os pilares de segurança da informação. Após a análise, foi possível constatar que a segurança é um dos desafios técnicos que precisam ser verificados, para que medidas adequadas de mitigação e recuperação possam ser implementadas, principalmente para as vulnerabilidades dos ataques.

Referências

Altawy, R. and Youssef, A. M. (2016). Security, privacy, and safety aspects of civilian drones: A survey. *ACM Trans. Cyber-Phys. Syst.*, 1(2):7:1–7:25.

ANAC (2017). *REQUISITOS GERAIS PARA AERONAVES NÃO TRIPULADAS DE USO CIVIL RBAC-E nº 94*. Agência Nacional de Aviação Civil, Rio de Janeiro.

Constantinides, C. and Parkinson, P. (2008). Security challenges in uav development. In *2008 IEEE/AIAA 27th Digital Avionics Systems Conference*, pages 1.C.1–1–1.C.1–8.

DECEA (2015). *Voos de VANT (drones)*. Departamento de Controle do Espaço Aéreo, Rio de Janeiro.

Deligne, E. (2012). Ardrone corruption. *Journal in Computer Virology*, 8(1-2):15–27.

Dey, V., Pudi, V., Chattopadhyay, A., and Elovici, Y. (2018). Security vulnerabilities of unmanned aerial vehicles and countermeasures: An experimental study. In *2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID)*, pages 398–403.

Ebeid, E., Skriver, M., and Jin, J. (2017). A survey on open-source flight control platforms of unmanned aerial vehicle. In *2017 Euromicro Conference on Digital System Design (DSD)*, pages 396–402.

Gartner (2017). *Gartner Says Almost 3 Million Personal and Commercial Drones Will Be Shipped in 2017*. Stamford. Disponível em: <https://www.gartner.com/newsroom/id/3602317>. Acesso em: 29 may. 2018.

Hartmann, K. and Steup, C. (2013). The vulnerability of uavs to cyber attacks - an approach to the risk assessment. In *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, pages 1–23.

He, D., Chan, S., and Guizani, M. (2016). Communication security of unmanned aerial vehicles. *IEEE Wireless Communications*, 24(4):134–139.

He, D., Chan, S., and Guizani, M. (2017). Drone-assisted public safety networks: The security aspect. *IEEE Communications Magazine*, 55(8):218–223.

Humphreys, T. (2012). Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil gps spoofing. *Subcommittee on Oversight, Investigations, and Management of the House Committee on Homeland Security*, pages 1–16.

Javaid, A. Y., Sun, W., Devabhaktuni, V. K., and Alam, M. (2012). Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In *2012 IEEE Conference on Technologies for Homeland Security (HST)*, pages 585–590.

Krishna, C. G. L. and Murphy, R. R. (2017). A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*, pages 194–199.

Marshall, D. M., Shappee, E., Barnhart, R. K., and Hottman, S. B. (2011). *Introduction to Unmanned Aircraft Systems*. CRC Press, Boca Raton Florida, first edition.

Rodday, N. (2015). Exploring security vulnerabilities of unmanned aerial vehicles. *DACS Research Group University of Twente*, pages 1–95.

Vattapparamban, E., Güvenç, , Yurekli, A. , Akkaya, K., and Uluağaç, S. (2016). Drones for smart cities: Issues in cybersecurity, privacy, and public safety. In *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 216–221.

Yagdereli, E., Gemci, C., and Aktaş, A. Z. (2015). A study on cyber-security of autonomous and unmanned vehicles. *The Journal of Defense Modeling and Simulation*, 12(4):369–381.