ESCOLA NAVAL

talanteobiffaire

Departamento de Ciências do Mar

Francisco Miguel de Castro Hipólito Lopes

Defesa contra UAS *commercial off the shelf* no âmbito das operações de *Harbour Protection*

Dissertação para obtenção do grau de Mestre em Ciências Militares Navais,

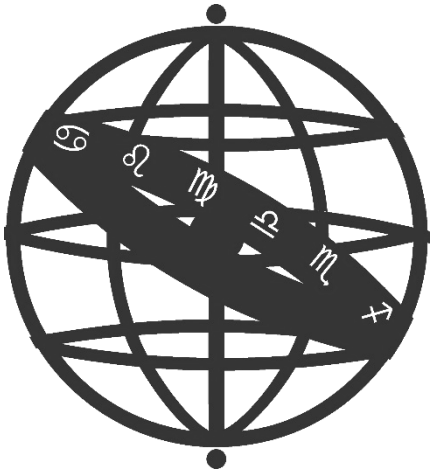
na especialidade de Marinha

Alfeite

2019

ESCOLA NAVAL

talante de bien faire



Francisco Miguel de Castro Hipólito Lopes

Defesa contra UAS comercial of the shelf *no âmbito das operações de* Harbour Protection

Dissertação para obtenção do grau de Mestre em Ciências Militares Navais,

na especialidade de Marinha

Orientação de: Professor Doutor Victor Lobo

Coorientação de: CTEN Nunes dos Santos

O Aluno Mestrando

ASPOF M Hipólito Lopes

O Orientador

Professor Doutor Victor Lobo

Alfeite

2019

Epígrafe

“ [The] most daunting problem [of 2016] was an adaptive enemy who, for a time, enjoyed tactical superiority in the airspace under our conventional air superiority in the form of commercially available drones and fuel-expedient weapons systems, and our only available response was small arms fire.”

- General Raymond A. Thomas III, Comandante do Special Operations Command maio de 2017

Dedicatória

Aos meus pais e à minha irmã, por todo o apoio na “retaguarda” prestado durante destes anos,

Aos meus amigos que sempre estiveram presentes ao longo do meu percurso, por todos os bons momentos

A todos, o meu sincero obrigado.

Agradecimentos

Gostaria de agradecer a todos os que, ao disponibilizarem o seu tempo e atenção, contribuíram de algum modo para a realização desta dissertação, nomeadamente:

Ao meu orientador, Professor Doutor Victor Lobo, por toda a ajuda e incentivo prestados ao longo da execução da dissertação;

Ao meu coorientador, Capitão-Tenente Nunes dos Santos, por coorientar a minha dissertação;

Ao Capitão-de-Fragata Anjinho Mourinha, por me ter apresentado esta temática e feito entender a pertinência da mesma;

Ao Tenente-Coronel Paulo Rosendo, por todos os conhecimentos que me transmitiu sobre a artilharia antiaérea no Exército Português;

Ao Capitão-Tenente Neves Simões, pela ajuda prestada no início da dissertação;

Ao Capitão-Tenente Cortes Banha e ao Major Pedro Ferreira, pelas entrevistas que me concederam;

Ao Capitão-Tenente Silva Ângelo, por todo o inestimável apoio prestado, sem o qual a realização desta dissertação teria sido bastante difícil;

Ao Primeiro-Tenente Mendes Lança e restante equipa da Célula de Experimentação Operacional de Veículos não tripulados, por me terem recebido na sua "casa" e mostrado o seu incrível trabalho;

Ao Primeiro-Tenente Seixas Nunes, pela colaboração durante os testes na Base Naval de Lisboa;

Ao Capitão João Chora e ao Primeiro-Sargento Joaquim Machado, pela partilha de conhecimentos sobre utilização de UAS no campo de batalha;

Às guarnições dos NRP *Álvares Cabral*, NRP *Vasco da Gama* e NRP *António Enes*, e à equipa do Centro de Investigação Naval, pelo apoio prestado durante os testes na Base Naval de Lisboa;

À câmara de oficiais e restante guarnição do NRP *D. Francisco de Almeida*, por todos os conhecimentos transmitidos durante o meu estágio nesse fantástico navio;

Aos meus camaradas, os Aspirantes a Oficial Costa Teles e Rodrigues Marante, por toda a ajuda, apoio e conselhos dados ao longo da realização desta dissertação.

Resumo

Nesta dissertação analisa-se a utilização de *Unmanned Aircraft Systems* (UAS) *Commercial off the shelf* (COTS) em ações de combate/terrorismo, enumeram-se as suas vantagens e desvantagens e define-se a potencial ameaça que representam no âmbito da *Harbour Protection* (HP). Abordam-se os sistemas *Counter*-UAS (C-UAS), percebendo como atuam sobre os UAS; e recolhe-se doutrina C-UAS já em vigor em forças militares.

Durante a realização desta dissertação foram efetuados testes reais com UAS e navios atracados na Base Naval de Lisboa, de modo a confirmar as capacidades dos sistemas atacantes e as reações a estes, e contribuiu-se para a elaboração das Táticas, Técnicas e Procedimentos (TTP) que estão a ser promulgadas na Marinha Portuguesa.

O resultado desta dissertação é uma proposta de medidas a adotar para ajudar a contrariar a utilização de UAS COTS em ações ofensivas contra navios atracados ou fundeados e unidades, instalações e infraestruturas localizadas nos portos.

Palavras-chave

Unmanned Aircraft Systems, Commercial off the shelf, Terrorismo, *Harbour Protection*, *Counter*-UAS

Abstract

On this dissertation, the usage of Unmanned Aircraft Systems (UAS) Commercial off the shelf (COTS) in combat/terrorism actions is analysed, referring its advantages and disadvantages, and the potential threat posed by it to Harbour Protection is defined. It is studied what are Counter-UAS (C-UAS) systems, understanding how they work against UAS, and it is gathered information about C-UAS doctrine already in use by military forces.

During this dissertation it had been executed real tests using UAS and warships moored at Lisbon Naval Base, in order to confirm the attacking systems' capabilities and the reactions against them, and it had been given some contribution to the elaboration of Tactics, Techniques and Procedures (TTP) that are being promulgated on Portuguese Navy.

This dissertation´s result is a proposal of some measures to be adopted in order to help to counteract the use of UAS COTS in offensive operations against moored or anchored ships and units, installations and infrastructures located in harbours.

Keywords

Unmanned Aircraft Systems, Commercial off the shelf, Terrorism, Harbour Protection, Counter-UAS

Índice

Epígrafe ..... **iii**
Dedicatória ..... **v**
Agradecimentos ..... **vii**
Resumo ..... **ix**
Palavras-chave ix
Abstract ..... **xi**
Keywords xi
Índice ..... **xiii**
Índice de Figuras ..... **xvii**
Índice de Tabelas ..... **xvii**
Lista de abreviaturas, siglas e acrónimos ..... **xix**
CAPÍTULO 1 - Introdução **1**
1.1 Enquadramento do Problema 1
1.2 Justificação do Tema 2
1.3 Objetivos da Dissertação 3
1.4 Questões da Investigação 3
1.5 Estrutura do Documento. 4
CAPÍTULO 2 – Enquadramento Teórico **5**
2.1 Introdução à Harbour Protection 5
2.1.1 Conceito de *Harbour Protection* e outros relacionados 5
2.1.2 Planeamento e condução das *Harbour Protection Operations* 8
2.2 Unmanned Aircraft Systems 10
2.2.1 Definição e Classificação 10
2.2.2 Breve História dos *Unmanned Aircraft Systems* 14
CAPÍTULO 3 - A ameaça do tipo *Unmanned Aircraft Systems Commercial Off-the-shelf* **19**
3.1 Porque podem os UAS COTS ser considerados uma ameaça. 19
3.1.1 UAS COTS como ameaça aos portos 19

3.1.2 Casos de utilização de UAS COTS 20
3.2 Definição da ameaça do tipo UAS COTS. 24
2.2.1 Pontos fortes e pontos fracos da sua utilização em ambiente de combate. 24
3.2.2 Formas de emprego 26
CAPÍTULO 4 – Sistemas C-UAS 31
4.1 O que são sistemas C-UAS 31
4.2 Princípios gerais do funcionamento dos sistemas C-UAS 32
CAPÍTULO 5 – Doutrina C-UAS 37
5.1 Análise do ATP 3-01.81 *Counter-Unmanned Aircraft System Techniques* 38
5.2 Análise do ATP 3-01.8 *Techniques for Combined Arms for Air Defense* .. 40
5.3 Análise do *Counter - Unmanned Aircraft System Strategy Extract* 42
CAPÍTULO 6 – A defesa contra UAS COTS no âmbito da HP 47
6.1 Táticas de utilização de UAS COTS contra HPO 47
6.1.1 Vigilância e recolha de informação. 49
6.1.2 Guerra eletrónica. 49
6.1.3 Ataques cinéticos 50
6.1.4 Interferência no espaço aéreo. 50
6.1.5 Transporte de material ilegal ou roubado. 51
6.1.6 Coordenação de ataques (C2). 51
6.1.7 "Ataque" não planeado 52
6.1.8 Ataque de enxame (saturação). 52
6.2 Casos particulares 53
6.2.1 Vigilância e aviso antecipado 53
6.2.2 *Rules of Engagement* 53
6.2.3 Contramedidas Passivas 54
6.2.4 Contramedidas Ativas 54
6.2.5 *Host Nation* 54
6.2.6 Sugestão de modelo a adotar por Unidades Navais nacionais em Condição Geral 5 – Navio atracado na BNL 54
CAPÍTULO 7 - Conclusão 57
7.1 Respostas à Questão Principal e Derivadas 57
7.2 Sugestões para trabalho futuro 58

Referências **59**

Apêndices **63**

Apêndice A – Relatório Técnico do Exercício com UAS comerciais na Base Naval de Lisboa, a 12 de fevereiro de 2019 ..... **63**

Índice de Figuras

Figura 1 - *Harbour Protection Areas*. Fonte ATP-94 6
Figura 2 – Etapas do Planeamento da HP. Fonte: ATP-94 8
Figura 3 - *Mission Analysis*. Fonte: ATP-94 8
Figura 4 - Hierarquia entre componentes de um UxS, de acordo com o RAMP. Fonte: Marques (2018) . 10
Figura 5 - *Main Blocks* de um UxS e seus sistemas. Fonte: Marques (2018) 11
Figura 6 - Fotograma retirado de um vídeo efetuado por um UAS COTS durante testes na BNL. Fonte: Apêndice A 27
Figura 7 - Durante a progressão de um elemento no terreno, o UAS acompanha-o de perto, enquanto faz o reconhecimento do percurso a seguir e vigia a sua retaguarda. 28
Figura 8- Exemplo de formato de relatório. Fonte: (US Army, 2016a) 42
Figura 9 - Principais linhas de ação. Fonte: (US Army, 2016a) 43
Figura 13 Imagem da Base Naval de Lisboa, obtida pelo Parrot Disco FPV. Note-se na posição 1 o NRP Vasco da Gama e na posição 2 o NRP António Enes. Fonte: UAS COTS operado pelos autores. 65
Figura 10 UAS COTS Parrot Bebop 2 FPV 65
Imagem 11 - UAS COTS Parrot Disco FPV 65
Imagem 12 - Imagem da Base Naval de Lisboa, obtida pelo Parrot Disco FPV. Note-se na posição 1 o NRP Vasco da Gama e na posição 2 o NRP António Enes. Fonte: UAS COTS operado pelos autores. 66
Figura 14 - Percurso realizado pelo Parrot Disco durante o exercício. Note-se que o mesmo foi lançado na posição1. 67

Índice de Tabelas

Tabela 1 - Classificação NATO de UAV. Fonte: Strategic Concept for UAS in NATO 12
Tabela 2 - Classificação do DoD de UAS. Fonte: DoD UAS *Airspace Integration Plan* 13
Tabela 3 - UAS comerciais utilizados no Iraque e na Síria. Fonte: Dan Gettinger. Imagens retiradas da Google. 22
Tabela 4 - Tipos e exemplos de táticas contra HPO utilizando UAS COTS. 48

Lista de abreviaturas, siglas e acrónimos

AAW – Anti-Air Warfare

ANAC – Autoridade Nacional de Aviação Civil

AOI – Area of Interest

AR – A Ré

ATP – Allied Tactical Publication

ATP – Army Techniques Publication

AV – Avante

AXP – Allied Exercise Publication

BB – Bombordo

BNL – Base Naval de Lisboa

C2 – Comando e Controlo

C4I – Command, Control, Communication, Computers and Intelligence

C4ISTAR – Command, Control, Communication, Computers and Intelligence, Surveillance, Target Acquisition and Reconnaissance

CBRN – Chemical, Biological, Radiological and Nuclear

CIA – Central Intelligence Agency

CIC – Combat Information Center

CITAN – Centro Integrado de Treino e Avaliação Naval

COMAR – Centro de Operações Marítimas

COP – Common Operational Picture

COTS – Commercial Off The Shelf

CS – Critical Spot

C-UAS – Counter - Unmanned Aircraft Systems

CWIS – Close-in-Weapon System

DoD – Department of Defense

EB – Estibordo

EI – Estado Islâmico

EME – Electromagnetic Environment

ETO – Equipamento de Transmissão de Ordens

EZ – Exclusion Zone

FARC – Fuerzas Armadas Revolucinoarias de Colombia

FCR – Fire Control Radar

FOC – Full Operating Capability

FPV – First-Person View

GLONASS – Global Navigation Satellite System

GNSS – Global Navigation Satellite System

GPS – Global Position System

HALE – High Altitude, Long Endurance

HAS – Harbour Safety Areas

HN – Host Nation

HP – Harbour Protetion

HPC – Harbour Protection Commander

HPL – Harbour Protection Levels

HPM – Harbour Protection Module

HPO – Harbour Protection Operations

HPROM – Harbour Protection Measures

IED – Improvised Explosive Device

ISR – Intelligence, Surveillance and Reconnaissance

JPC – Joint Force Commander

LSF – Low, Slow Flyers

LSS – Low, Slow and Small

LSS-UAS – Low, Slow and Small Unmanned Aerial Systems

MALE – Medium Altitude, Long Endurance

MP – Marinha Portuguesa

NATO – North Atlantic Treaty Organization

NBQ – Nuclear, Biológica e Química

NCIA – NATO Communications and Information Agency

NRP – Navio da República Portuguesa

ODN – Oficial de Dia ao Navio

PDE – Publicação Doutrinária do Exército

POCITAN –

PSP – Polícia de Segurança Pública

RAAA 1 – Regimento de Artilharia Antiaérea Nº 1

RCS – Radar Cross Section

RF – Radiofrequência

ROE – Rules of Engagement

RPA – Remotely Piloted Aircraft

SBAD – Surface-Based Air Defence

SLOC – Sea Lines of Communications

SPOD – Sea Port of Disembarkation

STANAG – Standardization Agreement

TAOR – Tactical Area of Responsibility

TCOR – Tenente-Coronel

TTP – Táticas, Técnicas e Procedimentos

UA – Unmanned Aircraft

UAS – Unmanned Aircraft Systems

UAV – Unmanned Aircraft Vehicle

UCAV – Unmanned Combat Aerial Vehicle

UCS – UAV Control Systems

CAPÍTULO 1 - Introdução

1.1 Enquadramento do Problema

Os *Unmanned Aerial Vehicle* (UAV) são cada vez mais utilizados à medida que o custo destes sistemas diminui e a sua popularidade aumenta (Bunker, 2015). Desde a fotografia à sua utilização como veículo de transporte, passando pelo simples lazer, o seu uso é cada vez mais diversificado. O mercado dos UAS *Commercial off-the-shelf*[1] (COTS) está em constante expansão e é dos mais promissores, tendo a *Federal Aviation Administration* estimado que até 2020 existam aproximadamente sete milhões de UAV, só nos Estados Unidos (Bliss, 2019).

Mas se os *Unmanned Aircraft Systems* (UAS)[2] prometem oferecer novas oportunidades, apresentam também novas ameaças à segurança (Wallace & Loffi, 2015). O seu baixo custo e a facilidade com que se adquirem torna-os atrativos para organizações terroristas e não-governamentais. O facto de não necessitarem de manutenção complexa e dispendiosa, ou do operador não precisar de treino específico, quando comparados com outros sistemas de armas, também ajuda a compreender a sua crescente popularidade no seio destes grupos. Quanto às missões que podem desempenhar, estas vão desde a simples recolha de imagens para efeitos de propaganda, à vigilância e reconhecimento, podendo também serem utilizados diretamente em ataques, com recurso a engenhos explosivos (Delgado, 2018). Uma vez que são cada vez mais pequenos e sofisticados, tornam-se também mais difíceis de detetar, identificar, seguir e destruir (NATO Air and Missile Defence Committee, 2018).

A preocupação com a possível utilização de UAS COTS para ações criminosas ou terroristas não é hipotética. Nos confrontos no Iraque e na Síria já foram identificados oito modelos diferentes de UAS comerciais utilizados pelas forças em combate (Gettinger, 2016). Esta preocupação é tal, que o Exército Americano considera os UAS

[1] Consideram-se *Commercial off-the-shelf* os produtos comercializáveis de fácil aquisição e normalmente usados sem sofrerem modificações (NATO, 2018).
[2] A referência a "*Aircraft*", em vez de "*Aerial*" como é usado na sigla UAV, está de acordo com as normas usadas em documentos NATO, e.g. (Joint Air Power Competence Centre, 2010).

dos grupos 1 e 2[3] como sendo o maior desafio contra as suas forças, uma vez que podem desempenhar várias funções de ataque (US Army, 2016a).

Como parte do seu papel na luta contra o terrorismo, a NATO está a desenvolver

meios para se defender contra o uso indevido de tecnologia pelos terroristas e propôs-se, como primeira prioridade, a contrariar a utilização de UAS por esses grupos (NATO Air and Missile Defence Committee, 2018). Também a Marinha Portuguesa está empenhada em desenvolver capacidades defensivas contra este tipo de sistemas (Marinha Portuguesa, 2018), tendo já testado, em exercícios, as suas capacidades contra esta nova ameaça.

1.2 Justificação do Tema

A capacidade que a NATO dispõe para projetar e sustentar operações afeta diretamente o seu sucesso. De modo a garantir uma eficaz resposta operacional, está fortemente dependente da liberdade de movimentos de abastecimentos, equipamentos e pessoal ao longo das *sea lines of communications* (SLOC). No entanto, assegurar a proteção das SLOC não é suficiente. Uma vez que mais de 90% de toda a carga militar chega a uma área de operações via *Sea Port of Disembarkations* (SPOD), os portos assumem-se como pontos chave para a mobilidade estratégica (NATO, 2017b).

Os portos de partida e os portos de chegada são, por si só, bastante vulneráveis. De modo a garantir a normal rotina de operações do porto, é necessário assegurar medidas protetivas dos navios (quer estejam a chegar, a sair, ou a operar dentro do porto), rotas de aproximação do porto, ancoradouros e infraestruturas críticas contra ameaças assimétricas (NATO, 2017b).

A ameaça assimétrica, definida como o uso de meios ou métodos capazes de contornar as forças do adversário, enquanto explora as suas fraquezas para obter um resultado desproporcional (NATO, 2017a), tem aumentado nos últimos anos. Existe a tendência, iniciada no final dos anos 80, e que continua nos dias de hoje, de se desenvolverem capacidades assimétricas como substitutos ou complementos das táticas convencionais (Exército Português, 2016). Conclui-se, portanto, que se vai verificar o

[3] UAS cujo peso é inferior a 20 libras (Grupo 1) e entre 21 e 55 libras (Grupo 2). Equivalem, pelos critérios NATO, à Classe I, Categoria
s Micro e Mini.

crescimento da utilização de armas de baixo custo e de elevada dissuasão, como os UAS. Tal se deverá a questões económicas, requisitos de formação e treino, fatores operacionais e a uma estratégia que pondera a dissuasão e razões de "custo *vs* eficácia" dos tradicionais meios aéreos (Exército Português, 2016).

As forças que por norma recorrem a ações compatíveis com a definição de ameaça assimétrica, e que tanto podem ser grupos terroristas como milícias governamentais, já demonstraram a capacidade de utilização de UAV (NATO, 2016). Não é, portanto, de todo descabido que se considere possível a utilização de UAS COTS como instrumento de ataque contra unidades navais num porto e instalações portuárias. Assim, torna-se necessário efetuar um estudo deste tipo de ameaça, para a melhor compreender, e propor conceito de defesa adequados, para melhor a contrariar.

1.3 Objetivos da Dissertação

O objetivo central desta dissertação é contribuir para a melhoria da defesa contra uma ameaça do tipo UAS COTS, no âmbito da *Harbour Protection* (HP). De modo a garantir que esse objetivo é cumprido, foram definidos os seguintes Objetivos Específicos (OE):

OE1 – Estudar a ameaça proporcionada por UAS COTS, analisando-a como tal e definindo-a;

OE2 – Recolher informação sobre sistemas *Counter*-UAS (C-UAS) COTS;

OE3 – Recolher e analisar exemplos de doutrina C-UAS já existentes;

1.4 Questões da Investigação

De acordo com os objetivos acima descritos, formulou-se a questão central:

Que doutrina deve ser elaborada para se melhor enfrentar a ameaça do tipo UAS COTS, no âmbito da HP?

Desta questão central definiram-se as seguintes Questões Derivadas (QD):

QD1 – Como se materializa a ameaça do tipo UAS COTS?

QD2 – Como funcionam os sistemas C-UAS COTS?

QD3 – Que doutrina C-UAS já existe e como pode ser adaptada para o caso específico dos UAS COTS?

1.5 Estrutura do Documento.

A presente dissertação possui a seguinte estrutura:

- Capítulo 1 – Introdução. Efetua-se um enquadramento da temática abordada, justificando a necessidade de efetuar o presente estudo. Expõem-se os Objetivos da Dissertação, as Questões da Investigação e apresenta-se a estrutura do documento.
- Capítulo 2 – Enquadramento Teórico. Apresenta-se os conceitos relacionados com *Harbour Protection* e UAS.
- Capítulo 3 – A ameaça do tipo UAS COTS. Analisa-se o porquê de os UAS COTS poderem ser considerados uma ameaça e define-se essa mesma ameaça.
- Capítulo 4 – Sistemas C-UAS. Explica-se o que são e como funcionam os sistemas C-UAS.
- Capítulo 5 – Doutrina C-UAS. Aborda-se a doutrina C-UAS já existente, com a intenção de retirar contributos para a elaboração de doutrina específica sobre C-UAS COTS.
- Capítulo 6 – A defesa contra UAS COTS no âmbito da HP. Este capítulo visa responder à questão central, tendo por base os conhecimentos retirados dos três capítulos anteriores.
- Capítulo 7 – Conclusão e Recomendações. Realiza-se um breve sumário dos resultados e uma análise dos mesmos, tendo em conta os objetivos inicialmente propostos. Responde-se às questões previamente elaboradas e apresentam-se sugestões para trabalhos futuros sobre este tema.

CAPÍTULO 2 – Enquadramento Teórico

Dois temas tão específicos, como a HP e os UAS COTS, necessitam de um cuidado enquadramento. Assim, este capítulo destina-se a apresentar os conceitos relacionados com a HP, de acordo com a publicação NATO ATP[4]-94 *Harbour Protection*, e com os UAS COTS, definindo-os, classificando-os e revendo a sua história.

2.1 Introdução à Harbour Protection

2.1.1 Conceito de *Harbour Protection* e outros relacionados

A publicação da NATO onde se aborda a *Harbour Protection* é o ATP-94. O seu propósito, de acordo com a mesma, é o de fornecer a filosofia, os princípios e as informações básicas sobre *Harbour Protection Operations* (HPO) e apresentar às Forças Expedicionárias da NATO uma base comum para a sua conduta, de modo a garantir proteção para unidades, instalações e infraestruturas, enquanto se mantêm as normais operações de rotina dos portos (NATO, 2017b).

A necessidade da existência de uma publicação específica nesta área advém da importância de se conseguir garantir a segurança dos portos. Estes adquirem especial valor, uma vez que mais de noventa por cento de todo o material militar chega à área de operações através de portos (*Sea Ports of Disembarkations*, SPOD) (NATO, 2017b). Torna-se, pois, indispensável assegurar que as operações normais dos portos não são afetadas, de modo a não comprometer as ações militares.

Assim, o conceito de *Harbour Protection* não é somente sobre garantir a segurança dos navios atracados no porto. Engloba as medidas de proteção e segurança às unidades, instalações e infraestruturas localizadas nos portos e ancoradouros associados utilizados em apoio a operações expedicionárias, enquanto se garante o normal funcionamento das operações portuárias. As áreas onde essas mesmas operações devem ser conduzidas, sempre com um risco mínimo, são designadas por *Harbour Safety Areas* (HSA) (NATO, 2017b).

[4] *Allied Tactical Publication*

A defesa de um porto ou de um ancoradouro e das suas aproximações pela água contra ameaças assimétricas/não convencionais externas entra no domínio da *Harbour Defence*. Já a salvaguarda de navios, portos, instalações e carga contra ameaças internas, como destruição, perdas e prejuízos provocados por sabotagem ou outros atos subversivos, acidentes, furtos ou outras causas de natureza semelhante, é considerada *Port Security*. A combinação das atividades de *Harbour Defence* e *Port Security* assume a designação de *Harbour Protection Operation* (HPO), e a área onde são conduzidas tem o nome de HP *Tactical Area of Responsibility* (HP TAOR) (Figura 1). Dentro da HP TAOR, existem pontos críticos (*Critical Spot*, CS), ou seja, áreas ou infraestruturas específicas que se forem afetadas podem comprometer o sucesso das HPO. Os CS podem englobar navios, cais, ancoradouros, instalações críticas, infraestruturas, etc (NATO, 2017b).

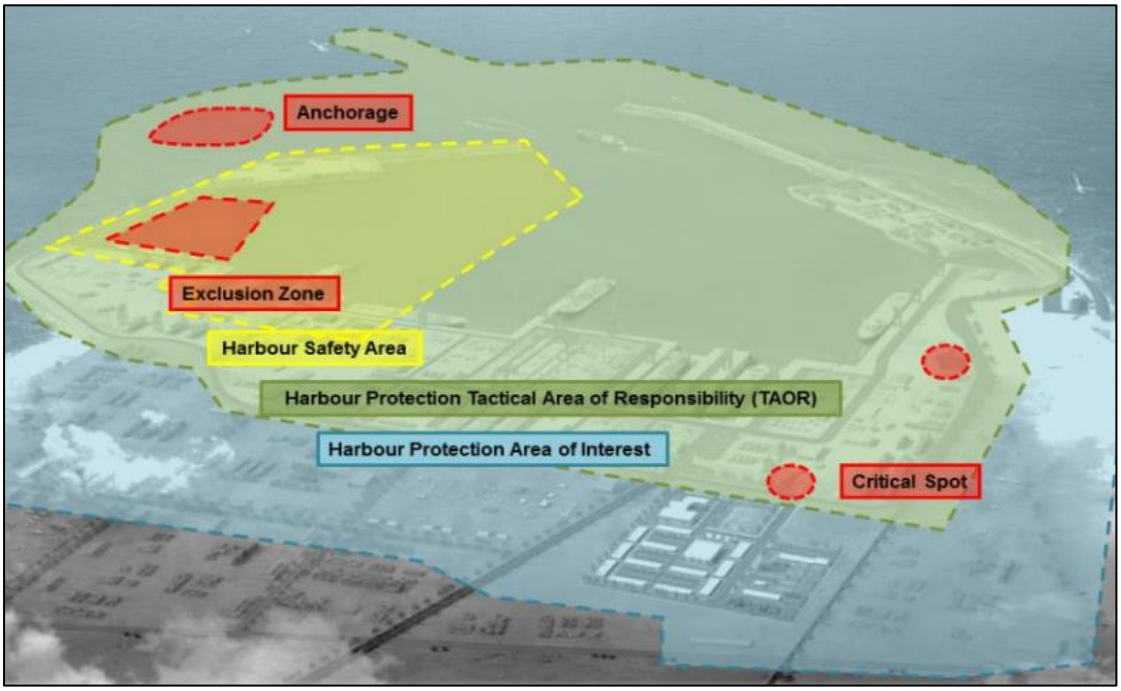


Figura 1 - *Harbour Protection Areas*. Fonte ATP-94

Se for necessário, podem ser criadas Zonas de Exclusão (*Exclusion Zones*, EZ). Estas são áreas sinalizadas e protegidas, perto ou dentro do porto, onde movimentos de civis são proibidos. O seu objetivo é o de limitar o mais possível o acesso a zonas sensíveis por parte de possíveis elementos terroristas ou criminosos, pois existem áreas de interesse (HP *Areas of Interest.* HP AOI), onde as ações do adversário podem afetar o resultado das operações de HP. Estas compreendem a TAOR, a HSA, a EZ, os CS e o *electromagnetic environment* (EME) envolvente (NATO, 2017b).

Para exercer o comando e controlo (C2) das forças empregues nas HPO existe um oficial responsável, designado por *Harbour Protection Commander* (HPC). O HPC tem de ser capaz de detetar, classificar, identificar e seguir meios aéreos, de superfície e de subsuperfície, e deve empregar os seus recursos numa defesa por camadas, enquanto coordena as forças de apoio dentro da HP TAOR. É ele quem estabelece ou altera os níveis de HP, e implementa as *Harbour Protection Measures* (HPROM) (NATO, 2017b).

De modo a auxiliar o HPC, bem como as forças que lhe estão atribuídas, na deteção, monitorização e resposta a ameaças assimétricas tridimensionais dentro da HP TAOR, foi desenvolvido o conceito do *Harbour Protection Module* (HPM). Este é um sistema integrado, destacável, modular, interoperável e blindado, que pode ser utilizado em terra ou embarcado num navio (atracado ou ancorado). O seu núcleo consiste num CIC guarnecido, com um Sistema de Gestão de Informação e Direção de Combate, comunicações e sensores, criando um sistema C4ISTAR[5] capaz de ajudar a construir a HP *Common Operational Picture* (HP COP) 24 horas por dia, 7 dias por semana (Figura 2) (NATO, 2017b).

Figura 2 - Exemplo de Harbour Protection Module. Fonte: ATP-94

[5] *Command, Control, Communication, Computers and Intelligence, Surveillance, Target Acquisition and Reconnaissance*

Considera-se que a HP está na sua total capacidade operacional (*Full Operating Capability*, FOC) quando o HPM está em contacto com todos os elementos da HPO, existe uma imagem operacional comum (*Common Operational Picture*, COP[6]) e esta pode ser mantida, e o HPC está pronto a cumprir todas as tarefas que lhe foram atribuídas e é capaz de assumir as responsabilidades dentro da HP TAOR (NATO, 2017b).

2.1.2 Planeamento e condução das *Harbour Protection Operations*

O HPC deve, desde o início, estar envolvido no processo de planeamento da HP. Este inclui vários passos, como a análise da missão, a identificação dos meios que são vitais para o cumprimento da missão, a definição da ameaça mais provável, a avaliação das vulnerabilidades de infraestruturas e instalações que possam ser exploradas por forças adversárias, a avaliação e a gestão do risco, a resposta ao incidente e a recuperação do mesmo (Figura 3). O planeamento da HP deve ter em consideração a situação, informações, recursos, a atribuição de sensores e fatores do ambiente envolvente, como por exemplo condições meteorológicas e tráfego marítimo (NATO, 2017b).

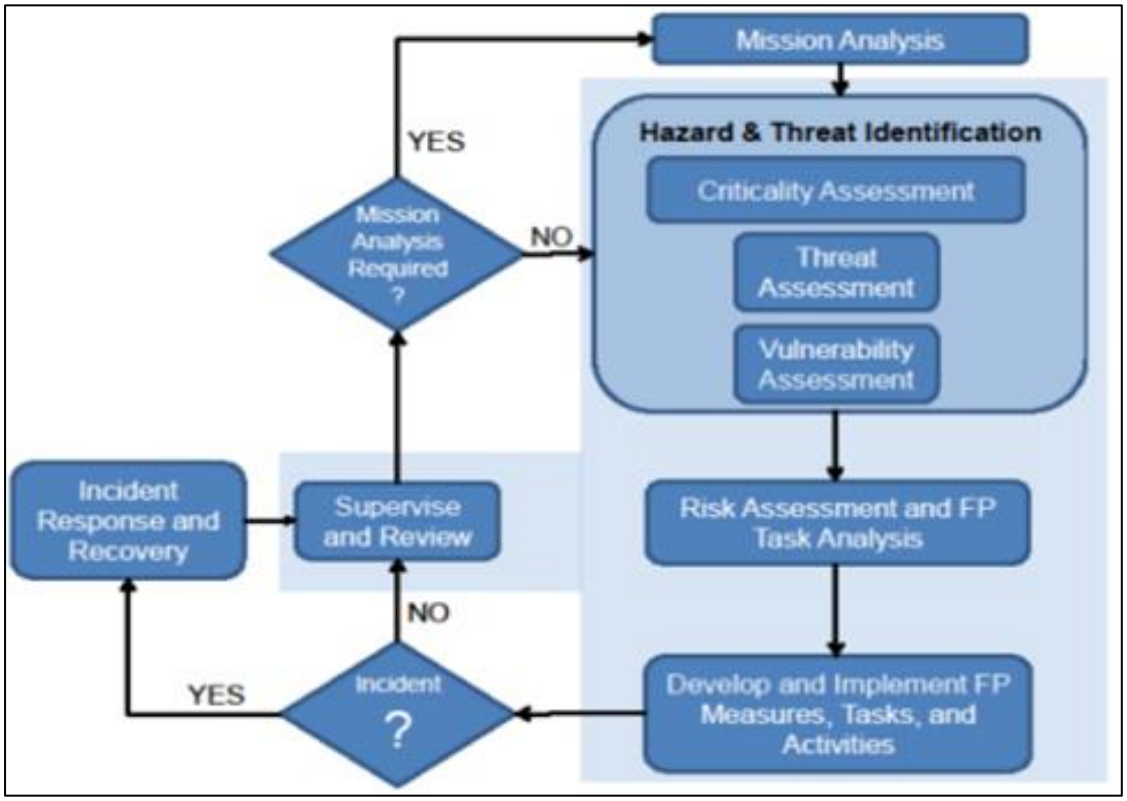


Figura 3 - *Mission Analysis*. Fonte: ATP-94

[6] *Common Operational Picture* é a imagem da situação operacional adaptada às necessidades do utilizador, baseada em informação comum partilhada por mais do que um comando (NATO, 2018).

A execução das HPO exige uma estrutura de comando e controlo robusta, uma vez que é muito complexa e envolve vários ambientes. Desse modo, é fundamental que o HPM contenha sistemas de C4I e que opere 24/7, com pessoal devidamente formado na operação e manutenção desses mesmos sistemas. Com as capacidades do HPM, o HPC deve de ser capaz de detetar, classificar/identificar e seguir objetos aéreos, de superfície e subsuperfície (NATO, 2017b).

Antes de se dar início a uma HPO, é necessário que um conjunto de pré-condições já esteja estabelecido, como por exemplo existência de redes de comunicações, instalações médicas, abastecimentos de comida e água, rotas de acesso ao porto limpas de engenhos explosivos, entre outros. O objetivo é criar uma aérea segura e otimizada, em terra e no mar, de modo a facilitar a implementação da HPO (NATO, 2017b).

Depois de estabelecidas as pré-condições necessárias, o HPC deve focar-se na implementação das fases de operação definidas durante o processo de planeamento. Uma HPO pode ter quatro fases. Em cada uma, o HPM, o HPC e as forças sobre o seu comando têm tarefas específicas atribuídas (NATO, 2017b).

A coordenação da HP é obtida através de níveis de HP (HP *Levels*, HPL) e de medidas de proteção (HP *Protection Measures*, HPROM), ordenados pelo HPC de acordo com o nível de ameaça esperado. Existem cinco níveis de HP e estes são conjuntos de medidas implementadas de modo a aumentar a vigilância e reduzir o risco. As HPROMS são níveis de HP, que vão desde o planeamento básico até ao mais detalhado, tendo em conta a prontidão, pessoal, armamento e medidas de proteção (NATO, 2017b).

De modo a ajudar o HPC a definir as opções de ação que tem à sua disposição, este deve receber as regras de empenhamento (*rules of engagement*, ROE) antes do início da primeira fase de HP. As ROE são instruções que definem as circunstâncias e limitações do uso de força. Devem estar de acordo com as leis nacionais e internacionais, sem nunca limitar o direito de agir em própria defesa. As ROE são implementadas pelo comandante da força (*Joint Force Commander*, JFC) e cabe ao HPC agir de acordo com elas (NATO, 2017b).

Os países onde os portos se situam (Host Nation, HN), são um fator importante em qualquer operação. Estas normalmente esforçam-se para fornecer a necessária segurança aos navios que atracam nos seus portos e tentam evitar que neles ocorra

qualquer tipo de ataque. É, pois vital que se crie uma ligação de cooperação com as autoridades da HN (NATO, 2017b).

2.2 Unmanned Aircraft Systems

2.2.1 Definição e Classificação

De acordo com a NATO (2018) *Unmanned Aircraft System* é um sistema cujos componentes incluem a aeronave não tripulada, a estrutura de apoio e todo o pessoal e equipamento necessários para controlar a aeronave não tripulada. Nesta dissertação é utilizada esta definição.

Existem vários modelos que descrevem os componentes de um UAS e como estes interagem. Um modelo particularmente útil, desenvolvido por professores da Escola Naval, é o *Refence Advanced Model from Portugal* (RAMP). Este, segundo Marques (2018), organiza os vários componentes de um sistema não tripulado (UxS) numa estrutura hierarquizada, dividida entre blocos principais (*main blocks*, MB), sistemas principais (*main systems*, MS) e subsistemas (*sub-systems*, SS) (Figura 4).

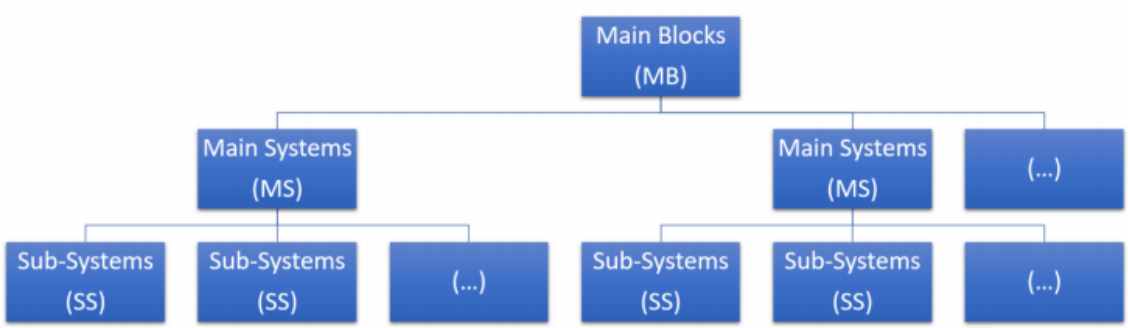


Figura 4 - Hierarquia entre componentes de um UxS, de acordo com o RAMP. Fonte: Marques (2018)

De acordo com o RAMP, existem três MB (Figura 5):

- MB1 – Veículo. Inclui o que normalmente se encontra a bordo do veículo, como *payload*, sistemas de navegação, sensores, subsistemas de comunicação, energia e propulsão. Nos casos em que o veículo está sob controlo remoto direto, certos subsistemas, como navegação, podem se encontrar fisicamente no *GroundSegment*.

- MB2 – *Datalink*. Inclui tudo o que integra a estrutura de comunicação. É estabelecida uma ligação entre o veículo e a estação de controlo através dos seus subsistemas de comunicação. Podem também ser estabelecidas comunicações com outros veículos e múltiplas estações em terra.
- MB3 – *GroundSegment*. Inclui todos os componentes físicos que estão fora do veículo. Normalmente encontram-se em terra, mas podem estar a bordo de um navio, uma aeronave ou em qualquer outro local. Por norma é constituído pelo equipamento de lançamento e recolha, equipamento de apoio, estação de controlo e um subsistema de comunicação

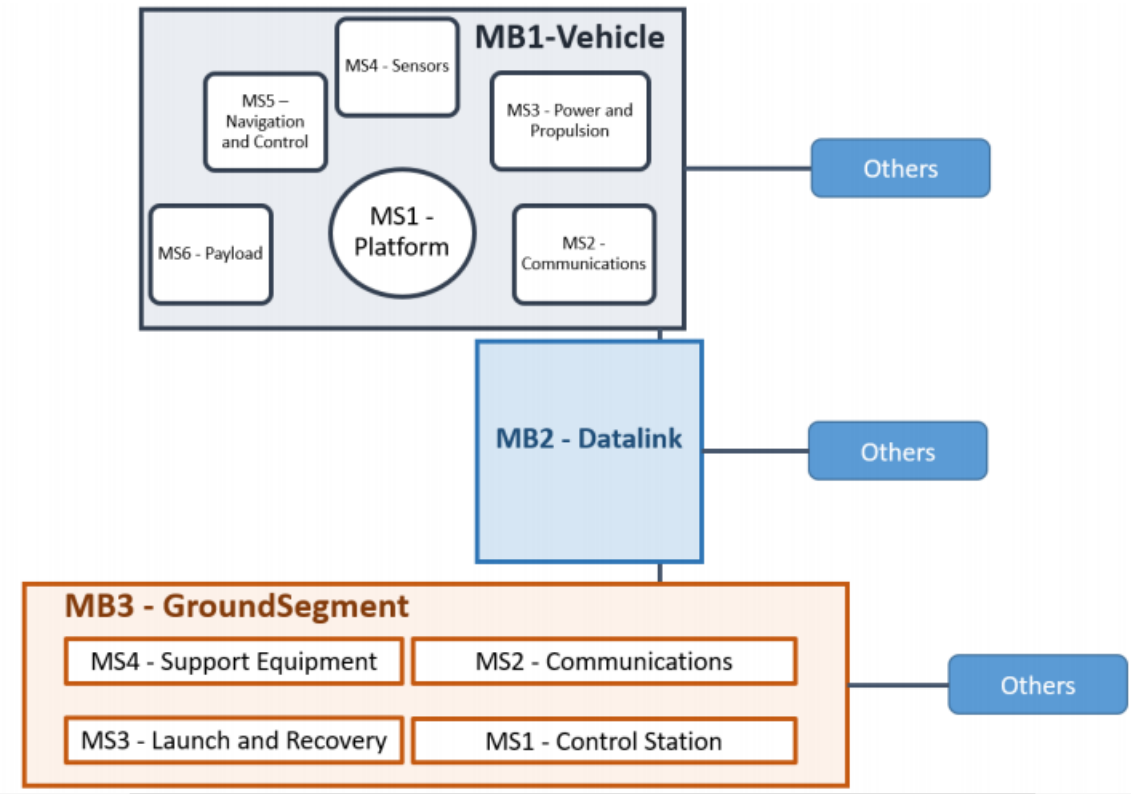


Figura 5 - *Main Blocks* de um UxS e seus sistemas. Fonte: Marques (2018)

O segundo nível do RAMP é o dos *Main Systems*. Estes são os elementos que compõe os *Main Blocks* e estão associados a cada um, onde normalmente se localizam fisicamente. Por exemplo, os sensores são um dos MS do MB "veículo", enquanto que a estação de controlo é um dos MS do MB "*GroundSegment*".

Os *Sub-systems* formam o terceiro nível do RAMP, sendo que estes elementos integram os *Main Systems*. Assim, os sensores de imagem são um SS do MS "sensores".

Os UAS podem ser classificados tendo em conta o seu peso, a altitude a que operam e o tipo de asa (se é rotativa ou fixa) (Marques, 2018). A NATO divide-os em três classes, de acordo com o seu peso. Na Classe I são agrupados os UAS com peso inferior a 150 kg. Os que têm entre 150 kg a 600 kg pertencem à Classe II e são considerados UAS táticos. Com mais de 600 kg, são UAS de Classe III, sendo que nesta categoria incluem-se os UAS de combate (*Unmanned Combat Aerial Systems*, UCAS) (Ver tabela 2).

Class	Category	Normal employment	Normal Operating Altitude	Normal Mission Radius	Primary Supported Commander	Example platform
CLASS I (less than 150 kg)	SMALL >20 kg	Tactical Unit (employs launch system)	Up to 5K ft AGL	50 km (LOS)	BN/Regt, BG	Luna, Hermes 90
	MINI 2-20 kg	Tactical Sub-unit (manual launch)	Up to 3K ft AGL	25 km (LOS)	Coy/Sqn	Scan Eagle, Skylark, Raven, DH3, Aladin, Strix
	MICRO <2 kg	Tactical PI, Sect, Individual (single operator)	Up to 200 ft AGL	5 km (LOS)	PI, Sect	Black Widow
CLASS II (150 kg to 600 kg)	TACTICAL	Tactical Formation	Up to 10,000 ft AGL	200 km (LOS)	Bde Comd	Sperwer, Iview 250, Hermes 450, Aerostar, Ranger
CLASS III (more than 600 kg)	Strike/ Combat	Strategic/National	Up to 65,000 ft	Unlimited (BLOS)	Theatre COM	
	HALE	Strategic/National	Up to 65,000 ft	Unlimited (BLOS)	Theatre COM	Global Hawk
	MALE	Operational/Theatre	Up to 45,000 ft MSL	Unlimited (BLOS)	JTF COM	Predator B, Predator A, Heron, Heron TP, Hermes 900

Tabela 1 - Classificação NATO de UAV. Fonte: Strategic Concept for UAS in NATO

Uma vez que nesta dissertação são abordadas publicações e doutrinas das Forças Armadas Americanas, importa referir qual a classificação utilizada pelo Departamento de Defesa (*Department of Defense*, DoD) dos Estado Unidos, que classifica os UAV em cinco grupos (Tabela 3) de acordo com o seu peso, altitude a que operam e velocidade (US Army, 2017).

Os grupos 4 e 5 contêm os maiores sistemas, normalmente utilizados para conduzir missões operacionais ou estratégicas. Operam a altitudes superiores a 18 000 pés e requerem pistas ou estradas para serem lançados. Os UAS dos grupos 2 e 3 são mais pequenos, com missões vocacionadas para as operações táticas. UAS do grupo 3

normalmente operaram nas altitudes dos grupos 4 e 5, mas não têm capacidade de transportar carga. UAS do grupo 2 operaram a menor altitude, abaixo dos 3 500 pés, têm uma limitada capacidade de transporte de carga e requerem algum suporte logístico. UAS do grupo 1 consistem em pequenos ou microssistemas que são facilmente empregues à vista do operador e são usados principalmente para vigilância e reconhecimento a baixa altitude, abaixo dos 1 200 pés (US Army, 2016a).

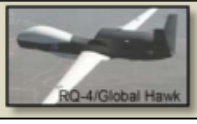
<table>
<tr><th>UAS Groups</th><th>Maximum Weight (lbs) (MGTOW)</th><th>Normal Operating Altitude (ft)</th><th>Speed (kts)</th><th colspan="2">Representative UAS</th></tr>
<tr><td>Group 1</td><td>0 – 20</td><td><1200 AGL</td><td>100</td><td>Raven (RQ-11),
WASP</td><td>  </td></tr>
<tr><td>Group 2</td><td>21 – 55</td><td><3500 AGL</td><td rowspan="2">< 250</td><td>ScanEagle</td><td>  </td></tr>
<tr><td>Group 3</td><td>< 1320</td><td rowspan="2">< FL 180</td><td>Shadow (RQ-7B),
Tier II / STUAS</td><td>  </td></tr>
<tr><td>Group 4</td><td rowspan="2">>1320</td><td rowspan="2">Any Airspeed</td><td>Fire Scout (MQ-8B, RQ-8B),
Predator (MQ-1A/B),
Sky Warrior ERMP (MQ-1C)</td><td>  </td></tr>
<tr><td>Group 5</td><td>> FL 180</td><td>Reaper (MQ-9A),
Global Hawk (RQ-4),
BAMS (RQ-4N)</td><td>  </td></tr>
</table>

Tabela 2 - Classificação do DoD de UAS. Fonte: DoD UAS *Airspace Integration Plan*

A maioria dos UAS COTS pode ser considerada como sendo do tipo *low, slow and small* (LSS). Um LSS UAS voa a baixas altitudes (menos de 4 km), move-se a baixas velocidades (menos que 50m/s) e é pequeno (pesa menos que 20 kg) (Dudush, Tyutyunnik, Trofymov, Bortnovs'kiy, & Bondarenko, 2018), o que faz com que se enquadre nas categorias mini e micro da Classe I (classificação da NATO). O Exército Americano considera que entram na categoria de LSS UAS os UAS pertencentes aos Grupos 1, 2 e 3 (US Army, 2017).

De acordo com Austin (2010), citado por Garcia (2015), os micro UAV têm uma envergadura inferior a 150 mm e são utilizados principalmente em zonas urbanas. O seu voo é lento e costumam ter um sítio onde aterrar ao longo do seu percurso, como um muro. Podem ser lançados com a mão e não são capazes de transportar cargas pesadas. Já os mini UAV, segundo o mesmo autor, são aeronaves capazes de serem lançadas manualmente, com peso inferior a 20 kg e que operam a uma distância de até 30 km.

Apesar do seu pequeno tamanho e da sua limitada capacidade de transporte de carga, são estes UAV que apresentam as maiores dificuldades para uma defesa mais consistente (US Army, 2016b).

Os links de comando dos UAS COTS normalmente operam nas bandas de frequência dos 2.4 GHz e dos 5.8 GHz (Dudush et al., 2018).

2.2.2 Breve História dos *Unmanned Aircraft Systems*

Os UAS surgiram na Primeira Guerra Mundial, quando a componente aérea dos exércitos se baseava em balões de ar quente e em primitivos aviões[7] (Blom, 2010), com cientistas e técnicos de países como os Estados Unidos e a Grã-Bretanha a desenvolverem aeronaves controladas por rádio (Bunker, 2015). Contudo, eram pouco fiáveis e despenhavam-se frequentemente (Gusterson, 2017).

Em 1917 Elmer Sperry aceitou uma proposta da Marinha Americana para a construção de um torpedo aéreo (Blom, 2010). De modo a conseguir fazer com que esse torpedo operasse sem necessitar de controlo humano, Sperry desenvolveu um giroscópio capaz de manter uma aeronave nivelada durante o voo. Esse equipamento tinha um dispositivo que fazia com que a aeronave "mergulhasse" sobre o alvo depois de ter percorrido uma determinada distância. Para colocar o torpedo voador no ar, optou por uma catapulta. No entanto, os testes realizados para demonstrar a eficácia do torpedo voador não foram satisfatórios. Embora a marinha tenha continuado com o programa depois da guerra, em 1922 cancelou-o (Blom, 2010, p. 25)

Também o exército americano tentou desenvolveu um torpedo voador. Em 1918, Charles Kettering criou um protótipo, que ficaria conhecido como *Kettering Bug* (Blom, 2010). Tinha um contador incorporado, que contabilizava o número de rotações do propulsor e cortava a energia do motor quando fosse atingido um número de rotações pré-determinado, fazendo com que o torpedo se despenhasse sobre o alvo. A guerra terminou antes que pudesse ser utilizado em combate (Blom, 2010).

[7] As principais funções táticas, tanto dos balões de ar quente, como dos aviões, eram reconhecimento visual, fotografia aérea e correção dos disparos da artilharia (Blom, 2010).

Os ingleses construíram vários UAV durante o período entre guerras, usados tanto como bombas voadoras como alvos para a prática de artilharia antiaérea. Um dos modelos, o *Fairley Queen*, foi utilizado com sucesso para treino dos artilheiros da Marinha Inglesa, levando a Marinha Americana a desenvolver um projeto semelhante.

Em 1938 a Marinha Americana tinha já um modelo controlado por rádio, acrescentando-lhe nos anos seguintes uma câmara de televisão e um torpedo. O objetivo era, assim que o operador detetasse um navio inimigo, utilizar o circuito de televisão para guiar o UAV contra o alvo e então libertar o torpedo. No entanto, durante a Segunda Guerra Mundial, o programa de desenvolvimento de UAV foi cancelado, em detrimento de um maior investimento na aviação convencional (Blom, 2010).

O Exército Americano também desenvolveu um UAV, o RP-4, que durante a Segunda Guerra só foi utilizado como alvo. No entanto, depois da guerra, o exército adaptou-o e transformou-o no seu primeiro UAV de reconhecimento (Blom, 2010).

Os alemães também investiram numa tecnologia similar, com as suas "bombas voadoras" V-1 e V-2 a atingirem cidades inglesas durante a guerra (Bunker, 2015). Estes sistemas consistiam em mísseis de cruzeiro com sistemas de orientação inercial (Oliveira, 2016).

Depois da Segunda Guerra Mundial, o Exército Americano utilizou aviões B-17 guiados por controlo remoto para analisar as nuvens cogumelo nos primeiros ensaios nucleares pós Hiroxima e Nagasáqui (Gusterson, 2017).

Durante a guerra fria, a investigação na área dos UAV continuou. O Exército Americano utilizou-os no Vietnam em missões de reconhecimento, enquanto que a Marinha os usava para dirigir os bombardeamentos dos seus navios (Blom, 2010).

Na década de 70, Israel começou a desenvolver o seu próprio programa de UAV, apresentando, em 1978, o *Mastiff Mk I* (Blom, 2010). Em 1982, durante a batalha de Bekaa Valey, utilizou UAV para acionar o sistema de defesa aéreo sírio (instalado no Líbano), que lançou os seus misseis contra os UAV. Enquanto os sírios recarregavam as suas peças, uma vaga de ataque de caças israelitas lançou os seus próprios mísseis e destruiu por completo o sistema de defesa aéreo sírio (Bunker, 2015).

Um projeto conjunto entre os Estados Unidos e Israel resultou no RQ-2 *Pioneer*, que viria a ser utilizado com resultados bastante satisfatórios nas operações Escudo do

Deserto e Tempestade do Deserto (Blom, 2010). As suas missões passavam pelo reconhecimento do campo de batalha e por missões de aquisição de alvo, sendo por vezes utilizados para lançar folhetos de propaganda (Bunker, 2015).

Ao longo das décadas de 1980 e 1990, a *Central Intelligence Agency* (CIA) apostou no seu próprio programa de UAV, o *Predator*, que viria a operar nos Balcãs (Bunker, 2015). Devido ao desenvolvimento do GPS e ao aumento da quantidade de dados capazes de serem transmitidos via satélite de e para os UAV, o *Predator* podia ser operado a milhares de quilómetros de distância. Ainda não transportava mísseis, sendo as suas missões o reconhecimento e a "iluminação" de alvos no solo através de *lasers*. Só em fevereiro de 2001 é que se testou o disparo de um míssil *Hellfire* a partir de um *Predator*, demonstrando ser possível lançar uma arma mais potente sem destruir a plataforma lançadora (Gusterson, 2017).

Com a invasão do Afeganistão em 2001, resultado do ataque terrorista do 11 de setembro, os UAV viram a sua utilização aumentar. Se antes destes acontecimentos, estavam no ativo, nas forças armadas americanas e agências de informação, menos de 50 unidades deste tipo, em 2012 eram já 7 494 (Bunker, 2015). A proporção de aeronaves pilotadas por controlo remoto na frota americana passou de cinco por cento em 2005 para trinta e um por cento em 2012 (Gusterson, 2017).

Atualmente, os UAS são utilizados por vários países, e operam em vários campos de batalha, como os do Iraque e da Síria. Os principais motivos que tornam os UAS tão apetecíveis pelos militares americanos são quatro. Primeiro, por serem melhores que satélites e aeronaves tripuladas em missões de reconhecimento. Segundo, por diminuírem a vulnerabilidade do operador e reduzirem as baixas das forças aliadas. Em terceiro lugar, os UAV são mais baratos do que as outras aeronaves[8]. Por fim, os UAV, devido à sua capacidade de vigilância por vídeo e aos mísseis guiados por laser que transportam, são extremamente precisos nos ataques que efetuam (Gusterson, 2017).

Em meados da década de 2000, os UAV "invadiram" o mercado civil. O grande interesse por parte de empresas e particulares, aliado aos custos da tecnologia inerente cada vez mais baixos, permitiu transformar esta arma militar numa ferramenta de trabalho e de lazer. A sua versatilidade ajuda a explicar o seu grande sucesso. Os UAV COTS são

[8] Um *Predator* custa cerca de 4,5 milhões de dólares americanos enquanto que um F-16 custa 47 milhões. (Gusterson, 2017)

utilizados para as mais variadas funções e não só como meio recreacional. As áreas profissionais onde são utilizados incluem o jornalismo, a monitorização de culturas, combate a incêndios, transportes, entre outros. A União Europeia estima que na próxima década os UAV atinjam 10% do volume de negócios no sector da aviação civil (Antunes, 2018) .

CAPÍTULO 3 - A ameaça do tipo *Unmanned Aircraft Systems Commercial Off-the-shelf*

Este capítulo contém dois subcapítulos. No primeiro expõe-se porque devem os UAS COTS ser considerados uma ameaça às operações normais dos portos, navios atracados ou fundeados e infraestruturas portuárias, e apresenta-se uma recolha genérica de ocasiões em que foram utilizados em ações terroristas ou de combate. No segundo subcapítulo, define-se a ameaça do tipo UAS COTS, enumerando os pontos fortes e fracos da sua utilização e que missões podem desempenhar.

3.1 Porque podem os UAS COTS ser considerados uma ameaça.

3.1.1 UAS COTS como ameaça aos portos

As operações no litoral, especialmente nos portos, são bastantes vulneráveis a ameaças convencionais e não convencionais/assimétricas, sendo precisamente estas últimas que apresentam o maior desafio no âmbito das HPO (NATO, 2017b).

Segundo Couto (1988), citado por Escorrega (2009), ameaça é "qualquer acontecimento ou ação (em curso ou previsível) que contraria a consecução de um objetivo e que, normalmente, é causador de danos materiais e morais". Já o termo "ameaça assimétrica" é mais específico, referindo-se às ações executadas com o objetivo de evitar ou negar ao adversário os seus pontos fortes, enquanto se explora as suas vulnerabilidades. Essas mesmas ações podem originar um resultado desproporcional e dar ao atacante uma vantagem que este poderia não ter obtido se tivesse recorrido a meios convencionais (NATO, 2017a).

As ameaças assimétricas são diversificadas e imprevisíveis, podendo-se materializar em atos de terrorismo e sabotagem, uso de armas de destruição massiva[9], ciberguerra e guerra da informação. Os engenhos explosivos improvisados[10] são a arma

[9] Armas de destruição massiva (*Weapon of Mass Destruction*, WMD), são armas capazes de causar uma enorme destruição e perda de vidas numa grande área (NATO, 2018).
[10] Engenhos explosivos improvisados (*Improvised Explosive Devices*, IED) são dispositivos fabricados de maneira improvisada e que incorporam químicos incendiários ou pirotécnicos letais. O seu objetivo é destruir, incapacitar, perturbar ou distrair. Podem incorporar material militar, mas normalmente usam componentes não militares (NATO, 2018).

de eleição, uma vez que são baratos, fáceis de contruir e de instalar no local a atacar (NATO, 2017b).

De acordo com o ATP-94 existem três tipos de ameaças aéreas assimétricas que são expectáveis que ocorram durante uma HPO: morteiros e rockets, *low slow flyers* (LSF) e UAV. Realça-se que não é feita nenhuma distinção específica entre as várias classes de UAV, podendo nesta definição incluir-se os UAS COTS, uma vez que os grupos terroristas estão, cada vez mais, a adotar tecnologias de índole comercial, das quais os UAS são um exemplo, de modo a planear, preparar e executar ataques contra forças da NATO e outras, suas aliadas (NATO Air and Missile Defence Committee, 2018).

Na realidade, a utilização de UAS COTS encaixa perfeitamente na definição de ameaça assimétrica. São "armas" baratas, que devido às suas características são capazes de evitar os meios de defesa do adversário, e conseguem transportar carga que pode provocar grande dano, como por exemplo IED ou substâncias químicas, biológicas, radiológicas e nucleares (*chemical, biological, radiological and nuclear*, CBRN).

3.1.2 Casos de utilização de UAS COTS

A ideia de utilizar um aparelho comercial, remotamente controlado, para infligir dano não é nova. A primeira tentativa (conhecida) de utilização de um UAS num atentado terrorista, foi efetuada pela seita japonesa Aum Shinrikyo[11], em junho de 1994, que pensou utilizar um helicóptero controlado remotamente para espalhar gás sarin. O helicóptero despenhou-se durante os testes, e a seita teve de recorrer a outros meios (Delgado, 2018).

Em agosto de 2002, o Exército Colombiano descobriu um acampamento das *Fuerzas Armadas Revolucionarias de Colombia* (FARC), organização paramilitar que usa táticas de guerrilha para enfrentar as forças governamentais. Nessa operação, descobriram-se nove aviões de controlo remoto, que se suspeita que seriam utilizados para transportar IED (Bunker, 2015).

Em 2004, a organização paramilitar islâmica Hezbollah realizou uma operação com UAS bem-sucedida. Usando um UAV fornecido pelo Irão, sobrevoaram Israel e

[11] Culto japonês apocalíptico, atualmente chamado *Aleph*, responsável pelo atentado no metro de Tóquio, em 1995, utilizando gás sarin. Por esse crime, o seu fundador, Shoko Asahara, e outros seguidores, foram executados.

conseguiram fazê-lo voltar para o Líbano sem serem descobertos (algumas versões sugerem que no voo de regresso, o UAV se despenhou no mar perto da costa síria). A 13 de agosto de 2006, três UAV carregados com entre quarenta a cinquenta quilogramas de explosivos foram abatidos por F-16 israelitas, sem conseguirem atingir os seus alvos (Bunker, 2015). Atualmente, o Hezbollah usa UAV para largar bombas sobre rebeldes sírios, no norte da Síria (Alami, 2017).

Outro grupo palestino, o Hamas, também tem utilizado UAS. Em novembro de 2012, a Força Aérea Israelita assegurou ter destruído oito UAV numa base do Hamas em Gaza, e em julho de 2014 terá abatido um UAV perto de Ashdod (Delgado, 2018). Também o Partido Islâmico do Turquestão e o *Jays Al-Fath* têm usado UAV em missões de reconhecimento ou para gravar batalhas para efeitos de propaganda (Delgado, 2018)

A organização que melhor soube transformar UAS em armas de combate foi o Estado Islâmico (EI). Ao contrário do Hezbollah, que teve apoio de outro país, o EI aproveitou a variada oferta de UAV comerciais, baratos e fáceis de adquirir. Utiliza-os para todo o tipo de missões, desde as de reconhecimento às de ataque, passando pelas de propaganda. Desde 2014 que o faz[12], tendo montado uma estrutura de apoio muito bem organizada, onde se incluem instalações de controlo, oficinas de reparação e adaptação, cadeias logísticas e centros de treino. Documentos capturados provam a extensão da sua burocracia, desde relatórios da utilização de UAV e listas de equipamento a recibos ou formulários de compra (Pomerleau, 2017). Para além disso, o EI, através da internet, fornece explicações sobre como modificar UAV comerciais e armá-los, de modo a que qualquer pessoa possa realizar ataques por todo o mundo (Delgado, 2018).

Dan Gettinger, no seu estudo *Drones Operating in Syria and Iraq*, faz a compilação dos UAV que operavam na Síria e no Iraque. O autor concluiu que pelo menos trinta e dois modelos distintos de UAV, fabricados em seis diferentes países, eram utilizados nesses dois países; a grande maioria sendo lançada manualmente ou por catapulta. Desses, oito são UAV de recreação. Foram também registados seis UAV não identificados, construídos artesanalmente. Dos UAV descritos nesse estudo, na tabela 3 estão destacados apenas os comerciais.

[12] As primeira vítimas mortais foram dois soldados curdos, a 2 de outubro de 2016 (Delgado, 2018)

Phantom		Produzido pela empresa chinesa DJI, é do tipo *quadcopter*. O Phantom 4 consegue desviar-se de obstáculos e seguir pessoas ou objetos (*Active Track*) devido aos seus múltiplos sensores. É utilizado pelas forças governamentais sírias e pelo EI.
Inspire		É um *quadcopter* da DJI, lançado com o objetivo de ser um meio-termo entre um UAV para profissionais ou para pura diversão. Acredita-se que seja utilizado pelas forças governamentais sírias.
F550 Flame Wheel		Outro UAV produzido pela DJI, este *hexacopter* é um kit para o operador montar. Desenhado para ser mais resistente que outros UAV, supõe-se ser utilizado pelas forças governamentais sírias.
Matrice 100		Também fabricado pela DJI, tem o dobro do tempo de voo de um Phantom e é utilizado pela Polícia Federal Iraquiana.
Skyhunter FPV		É um UAV de asa fixa fabricado pela companhia chinesa Tensho Model Co., Ltd. É utilizado pelo Estado Islâmico, tendo alguns UAV sido abatidos ou capturados.
Skywalker X8		Produzido pela chinesa *Guilin Feiyu Electronic Technology*, é um UAV de asa fixa, utilizado pelo Estado Islâmico
X-UAV Talon		UAV de asa fixa, fabricado pela HOOAH Aviation Technology Co., Ltd, e operado pelo EI.
My Twin Dream		Produzido pela MyFlyDream, é operado pelo Kurdish Peshmerga

Tabela 3 - UAS comerciais utilizados no Iraque e na Síria. Fonte: Dan Gettinger. Imagens retiradas da Google.

Segundo o mesmo autor, foi nestes conflitos que, pela primeira vez, UAV comerciais foram transformados em IED voadores. Mas embora a utilização de UAV por

grupos terroristas esteja ainda na fase experimental, está a aumentar, assim como a capacidade desses sistemas (Bunker, 2015).

Durante a Batalha de Mosul[13], dezenas de militares iraquianos foram mortos ou feridos por granadas ou explosivos leves largados por UAS COTS. Terá sido talvez a primeira vez desde a Guerra do Vietnam que as forças militares americanas estavam impotentes contra aeronaves inimigas (Arnold & Fiore, 2019).

Mais recentemente, a 4 de agosto de 2018, ocorreu uma tentativa de atentado contra o presidente da Venezuela, Nicolás Maduro, utilizando-se dois UAS COTS carregados com um total de cerca de dois quilos de explosivos. A intenção era uma das aeronaves explodir sobre o presidente, enquanto que a outra deveria rebentar à sua frente. No entanto, os militares venezuelanos conseguiram desviar um dos UAS COTS da sua rota através de meios eletrónicos e o outro despenhou-se contra um edifício de apartamentos (Kelly, 2018). Os UAS foram adquiridos online e armados com explosivos militares. Os operadores treinaram-se na utilização dos UAS numa quinta na Colômbia, tendo testado várias possibilidades, como lançarem-nos a partir da janela de um carro, durante a noite. Para atravessarem a fronteira, desmontaram os UAS e reconstruiram-nos mais tarde, na Venezuela. Segundo o responsável pelo ataque, este só não teve sucesso porque os UAS explodiram prematuramente, devido aos bloqueadores de sinal de telemóvel usados para proteger o presidente e que provocaram as explosões (Walsh et al., 2019).

Convém, ainda, aqui destacar dois casos de incidentes com UAS COTS, que embora não tenham sido causados por grupos criminosos ou terroristas, atestam a facilidade com que conseguem evitar medidas de segurança, e ajudaram a despertar a atenção para este tipo de ameaça.

O primeiro caso ocorreu em dezembro de 2013. Durante um comício partidário no qual participava, a chanceler alemã Angela Merkel viu um pequeno *quadcopter* voar e despenhar-se à sua frente. O UAS era operado por membros de um outro partido, que o utilizaram como protesto precisamente pela utilização de aeronaves não tripuladas pela Alemanha para efeitos de segurança (Wallace & Loffi, 2015).

[13] A Batalha de Mosul (2016-2017) foi uma operação militar para recuperar o controlo da cidade iraquiana de Mosul, que havia sido conquistada pelo Estado Islâmico em 2014 (Arnold & Fiore, 2019).

Em janeiro de 2015, um funcionário da *National Geospatial Intelligence Agency* perdeu o controlo do UAV de um amigo, um DJI Phantom FC40 , fazendo com que este se despenhasse nos relvados da Casa Branca (Walters, 2016). Embora a aeronave tenha sido avistada por um agente de segurança, não foi detetada pelos radares de defesa aérea da Casa Branca (Wallace & Loffi, 2015). O próprio agente não foi capaz de intercetar o UAV, que só parou quando bateu numa árvore (Walters, 2016).

3.2 Definição da ameaça do tipo UAS COTS.

3.2.1 Pontos fortes e pontos fracos da sua utilização em ambiente de combate.

Os UAS COTS, enquanto arma, têm os seus fortes e pontos fracos. A sua enumeração é importante, pois permite compreender como podem os UAS COTS ser utilizados, ajudando a definir quem os utiliza e a limitar o seu espectro de operações. Perceber as capacidades e limitações dos UAS aumenta a habilidade dos militares reagirem e derrotarem a ameaça (US Army, 2016a).

O seu principal ponto forte é o quão barato e fácil de adquirir são. Nos principais *sites* de venda *on-line* encontram-se facilmente UAV novos ou usados, ou peças para estes. A página da "Amazon" apresenta mais de 10 000 resultados de pesquisa para "*drone*" (Amazon, 2018b) e no "ebay" aparecem 490 998 produtos (Ebay, 2018). Por outro lado, os preços são acessíveis. Por exemplo, o Phantom 4 (UAV da 4ª série do modelo dos que têm sido utilizados pelo EI na Síria) custa apenas 899 dólares na Amazon (Amazon, 2018a). Encomendar é também um processo simples e relativamente rápido. O UAV anterior, encomendado nesse *site*, demora entre dois a três dias a estar pronto para entrega. Comprar peças à parte e depois montá-las é também uma opção, tendo em conta que no *Youtube* estão disponíveis vídeos que ensinam a construir UAV (Youtube, 2018b).

O seu segundo ponto forte é o de serem fáceis de operar. Ao contrário de outros sistemas de armas, que necessitam de um certo grau de treino e experiência, os UAS COTS são fáceis de operar. Acresce o facto de existirem cursos *on-line* para se aprender a pilotar UAV (Udemy, 2018) e vídeos no *Youtube* especialmente vocacionados para os amadores (Youtube, 2018a). O próprio UAV dispõe de uma série de ajudas para o utilizador. A maior parte dispõe de navegação por satélite (GPS/GLONASS), o que lhe permite seguir rotas pré-estabelecidas. Existem também os que têm um sistema de seguimento autónomo de pessoas ou veículos. (*Follow Me*, da marca Parrot (Parrot, 2018)

e *Active Track*, da DJI (DJI, 2018), por exemplo). Há os que têm a opção de anti colisão, com sensores que fazem com que o UAV se desvie de obstáculos. São também fáceis de transportar e armazenar.

Outro ponto forte é a furtividade que lhes está associada. O ser furtivo significa ser difícil de detetar e seguir. Os UAV reúnem um conjunto de características que lhes dão essa habilidade, tais como o seu reduzido tamanho (o que os torna difícil de serem detetados visualmente, mesmo a curtas distância), o pouco barulho que fazem (se estiverem equipados com motores elétricos), uma *Radar Cross Section* (RCS) pequena, e reduzida emissão de radiação infravermelha. (Exército Português, 2016). Todas estas capacidades dão-lhes uma grande vantagem tática, uma vez que lhes permitem aproximar-se do alvo sem serem detetados até que já estejam demasiado perto, e faz com que evitem facilmente os sistemas de defesa aérea convencionais

Os sensores eletro-óticos de que dispõem são mais um dos seus pontos fortes, pois esta característica fornece-lhes imagem em tempo real, aumentado assim a capacidade de C2, o que lhes possibilita coordenar ataques ou guiar o UAV até ao alvo. As imagens recolhidas podem também ser utilizadas para fins de propaganda (Delgado, 2018).

A sua versatilidade é também uma vantagem. Como utilizam o espaço aéreo para operar, podem realizar um conjunto de missões que estão negadas a um operador no solo. Podem, por exemplo, ultrapassar facilmente perímetros de segurança e fortificações, algo que é difícil para um bombista suicida ou um caminhão carregado de explosivos. A sua grande mobilidade aumenta-lhes essas capacidades, enquanto torna mais difícil a sua deteção e abate. A sua autonomia (normalmente medida em minutos de voo) é suficiente para permitir a realização de ataques rápidos e o seu alcance possibilita atingir alvos longe do operador, contribuindo para aumentar a sua segurança.

Outra vantagem é a salvaguarda da vida humana durante as operações. Uma vez que que os UAV são não tripulados e são remotamente controlados, possuem a vantagem de fornecer uma maior proteção ao operador.

Por fim, há também que te em conta o efeito psicológico que este tipo de ataques provoca (Dudush et al., 2018).

Relativamente aos seus pontos fracos, são identificados quatro, sendo de destacar o quão facilmente são afetados pelas condições ambientais. Os UAV são influenciados

pelos efeitos meteorológicos adversos, como a chuva, neve ou vento. Com nevoeiro, o voo não é afetado se seguir coordenadas pré-estabelecidas. Durante a noite as operações estão bastante limitadas. Uma câmara normal, sem capacidade de visão infravermelha, dificilmente distinguirá o alvo em zonas pouco iluminadas. E embora seja possível dotar os UAV com sensores térmicos ou sistemas de visão noturna, esses consumirão energia e reduzirão a sua autonomia (Delgado, 2018).

O seu segundo ponto fraco é a sua reduzida capacidade de transporte de carga, embora o peso que cada UAV pode transportar varia de modelo para modelo. Existem UAV especialmente desenhados para essa função e que são facilmente adquiridos[14], ou então os modelos normais podem ser modificados para ganhar essa característica. A capacidade de carga determina a quantidade e o tipo de explosivos transportados e, por inerência, o género de ataque. Normalmente transportam granadas de mão, munições de morteiros ou IED (Delgado, 2018). Há por isso que ter em conta que, embora a carga possa ser leva, esta pode ainda ser bastante perigosa.

Outra das suas fraquezas é a sua vulnerabilidade a ataques do tipo *jamming* e *spoofing* e há um investimento crescente no desenvolvimento de sistemas C-UAS que atuam nesta área.

O seu quarto ponto fraco é a fragilidade do material com que são construídos, sendo a maior parte de plástico e esferovite. Essa desvantagem faz com que não sejam suficientemente robustos para enfrentar mau tempo e caso sejam atingidos, a probabilidade de o operador conseguir recuperar o UAV é baixa.

3.2.2 Formas de emprego

Devido às características específicas que possuem, os UAS COTS podem ser utilizados numa variada gama de missões:

[14] O Walker, da Airborne Drones, é um bom exemplo de um UAV de transporte de carga.

a) Vigilância e recolha de informação, recorrendo aos seus sensores de imagem. Os UAS dos grupos 1 e 2, dos quais os COTS fazem parte, têm a capacidade de operar sem serem detetados e a curtas distâncias. Isso permite-lhes realizar uma vigilância detalhada, a partir de vários pontos de vista. É o mais provável modo de utilização, uma vez que permite o uso do UAS, sem este ser destruído (US Army, 2016a). Através da realização de testes (Apêndice A), o autor pôde comprovar esta capacidade (figura 4).

Figura 6 - Fotograma retirado de um vídeo efetuado por um UAS COTS durante testes na BNL. Fonte: Apêndice A

b) Guerra eletrónica, se transportarem um *jammer* ou *spoofer*.
c) Ataques cinéticos contra infraestruturas críticas ou altas entidades, recorrendo ao transporte de explosivos ou outro tipo de arma, que podem ser largados, ou executando ataques do tipo "*kamikaze*";
d) Interferência no espaço aéreo, por forma a destabilizar as operações de voo de aeronaves amigas (Wallace & Loffi, 2015). Mesmo sem transportarem qualquer tipo de armamento, os UAS COTS podem causar danos suficientemente graves se embaterem contra zonas sensíveis da aeronave. Testes recentes demonstraram que até os UAS mais pequenos conseguem penetrar nas asas e nos para-brisas dos aviões (Bliss, 2019). A sua simples presença nas imediações de aeroportos, ou de outras zonas de aterragem/descolagem de aeronaves, é o suficiente para cancelar as operações de voo. Segundo a Autoridade Nacional da Aviação Civil (ANAC), entre janeiro e setembro de 2018, foram registados 43 incidentes com UAV (Jornal

de Notícias, 2019). Por exemplo, a 19 de setembro de 2018, o aeroporto de Lisboa foi obrigado a interromper operações por onze minutos, levando a que dois aviões fossem desviados para Faro e que uma aterragem fosse interrompida. Embora tendo sido chamada ao local, a PSP não conseguiu identificar o operador (Agência Lusa, 2018).

e) Transporte de material ilegal ou roubado. Devido à sua facilidade de ultrapassar barreiras, como muros ou redes, os UAS têm vindo a ser utilizados para transporte de carga ilegal, como contrabando e outros. Por exemplo, nas prisões portuguesas têm ocorrido casos de utilização de UAS COTS para a introdução de material não permitido, como telemóveis, dentro dos estabelecimentos. Os guardas prisionais afirmam não terem a formação ou os equipamentos necessários para poderem combater estas situações (Observador, 2019). No caso específico da HP, os UAS podem ser utilizados para deixar um IED numa posição pré planeada, dentro do porto, de modo a mais tarde um cúmplice o ir buscar. Os UAS podem também ser utilizados para transportar material roubado para o exterior do porto.
f) Coordenação de ataques (C2). Uma vez que se consegue aceder às imagens captadas pelo UAS em tempo real, os lideres dos grupos de ataque são capazes de transmitir aos seus homens as posições e movimentações das forças de HP, qual o melhor caminho a seguir para alcançarem o alvo e quais as ameaças nas suas proximidades (Figura 7). Os UAS também podem agir como aparelhos de retransmissão de comunicações (US Army, 2016a).

Figura 7 - Durante a progressão de um elemento no terreno, o UAS acompanha-o de perto, enquanto faz o reconhecimento do percurso a seguir e vigia a sua retaguarda.

g) Ataque em enxame. Talvez o mais perigoso método de ataque, embora não o mais provável. Grupos de UAS podem ser utilizados de três maneiras diferentes (vigilância, ataque indireto e ataque direto). Podem ser pré-programados ou operados remotamente. Os grupos podem ser utilizados para perturbar as operações de reconhecimento da força adversária ou para destruir um ponto de controlo de entrada (US Army, 2016a).
h) "Ataque" não planeado, que ocorre devido a algum descuido do operador, ou quando existe algum problema nalgum dos componentes do UAS que faz com que o operador perca o controlo da aeronave, e esta provoque um acidente não intencionado.

Depois do ataque, os UAS COTS podem ainda servir para avaliar os danos provocados, permitindo aos atacantes perceber quais os resultados alcançados. Há igualmente que ter em consideração que as gravações dos ataques, embora não representem uma ameaça direta contra as forças amigas, podem ser utilizadas para efeitos de propaganda e para minar a moral dos seus adversários.

CAPÍTULO 4 – Sistemas C-UAS

Neste capítulo abordam-se os sistemas C-UAS, definindo-os e percebendo como funcionam.

4.1 O que são sistemas C-UAS

De um modo geral, sistemas C-UAS são sistemas utilizados especificamente para detetar e/ou intercetar UAS, tendo surgido devido às preocupações relativas à utilização de UAS e às ameaças que estes constituem, tanto para militares, como para civis (Michel, 2018). A NATO já identificou a importância de possuir um sistema desse tipo, tendo lançado, em junho de 2018, uma *Invitation for Bid* (IFB), com o objetivo de adquirir um sistema C-UAS, capaz de detetar e destruir, se necessário, pequenos UAS COTS, de asa fixa e rotativa, incluindo aqueles que não transmitissem sinais rádio ou que pudessem efetuar voos pré-programados (NATO Communications and Information Agency [NCIA], 2018). Também o Exército Português reconheceu a necessidade de adquirir um "sistema anti-drone" que pudesse ser operado pelo próprio em ações de policiamento aéreo, sob normativos da ANAC (Regimento de Artilharia Antiaérea Nº 1 [RAAA1], 2017).

A verdade é que a utilização de UAS COTS exige novos meios de defesa, com capacidades específicas de deteção e interceção. Tentar detetá-los visualmente não é muito eficaz, pois a uma distância de algumas centenas de metros, os UAV são praticamente invisíveis a olho nu. O autor da dissertação comprovou-o pessoalmente, durante um exercício realizado na Base Naval de Lisboa (ver apêndice A).

Os sistemas de defesa antiaérea normalmente utilizados contra aeronaves são, por norma, ineficazes contra este novo tipo de ameaça. Os radares estão desenhados para detetar objetos voadores grandes e rápidos, nem sempre sendo capazes de detetar objetos pequenos e lentos, que voam a baixas altitudes. A somar a esta incapacidade, há que ter em conta que os UAV não têm *transponder*, logo não podem ser detetados e seguidos pelos sistemas de controlo do espaço aéreo. Por fim, o custo de utilizar um míssil antiaéreo, que pode chegar aos milhares de euros, contra um UAV, de poucas centenas, não é razoável. Mesmo que se opte por o derrubar, não é assim tão fácil. A julho de 2016,

um UAV de asa fixa, de fabrico russo, que invadiu o espaço aéreo Israelita, sobreviveu a dois mísseis *Patriot* e a um míssil ar-ar lançado por um caça (Michel, 2018). Durante o exercício SWORDFISH18[15], onde se treinou a proteção de uma força contra ameaças aéreas assimétricas, quando em trânsito em águas litorais, embora se tenha efetuado fogo (de *browning*[16] e PHALANX[17]) contra os dois UAS utilizados para o efeito, nenhum foi abatido.

Todas estas razões levaram ao desenvolvimento de uma indústria especialmente vocacionada para a deteção e/ou derrube de UAV COTS. O seu crescimento foi extraordinário: de 10 sistemas C-UAS disponíveis no mercado em 2015 para mais de 200 menos de três anos depois. Estima-se que o seu valor de mercado possa atingir os 1.5 mil milhões de dólares em cinco anos (Michel, 2018).

No entanto, a tecnologia aplicada aos C-UAS não acompanhou o rápido desenvolvimento da tecnologia dos UAS da classe I, existindo ainda dúvidas sobre como os diferentes sistemas C-UAS se comportam em diferentes ambientes e contextos operacionais, qual a sua eficácia contra ameaças de vários tipos e como podem ser integrados noutros sistemas já existentes. Há também que ter em atenção a necessidade de evitar que estes sistemas interrompam as operações de UAS das próprias forças (NATO Air and Missile Defence Committee, 2018).

Os C-UAS têm vindo já a ser utilizados no âmbito militar para vigiar bases, como complemento a outros sistemas já existentes. Podem ser instalados em posições estáticas (como edifícios), montados noutros UAV ou serem móveis (como veículos). Podem também ser desenhados para serem portáteis e operados por um único indivíduo, como as *DroneGuns,* "armas" de fácil utilização que não necessitam de qualquer formação específica para a sua operação (Michel, 2018).

4.2 Princípios gerais do funcionamento dos sistemas C-UAS

Há vários estudos sobre como deve funcionar um sistema C-UAS, sendo que um deles, desenvolvido por Birch, Griffin e Erdman (2015), considera que existem três passos distintos. O primeiro é a deteção, ou seja, recolha de informação, obtida através

[15] Exercício naval bianual da Marinha Portuguesa.
[16] Metralhadora de calibre 12.7mm utilizada a bordo dos navios da Marinha Portuguesa.
[17] A PHALANX é um *Close-in-Weapon System* (CIWS), de calibre 20mm e utilizado a bordo das fragatas da classe Vasco da Gama. O seu principal objetivo é a defesa contra mísseis antinavio e aeronaves.

de um sensor, sobre um possível alvo. A seguir, efetua-se a classificação, analisando-se e filtrando a informação recolhida na fase anterior, de modo a apenas selecionar a informação relativa ao UAS. Por fim, e depois da confirmação positiva de que o que foi detetado na primeira fase é realmente um UAS, é necessário impedir que este consiga cumprir a sua missão (neutralização).

Outro modelo, o "*five kill chain"*, de Buric e Cubber (2017), apresenta cinco fases no combate a um UAS. Na primeira etapa, deteção, vários sensores, de diferentes tipos, estão ligados em rede e procedem à recolha de informação, de modo a melhor conseguirem detetar com a maior certeza, e no mais curto espaço de tempo, um UAS. Quando se detetar algo, ocorre a fase da classificação, onde a informação recolhida é analisada, de modo a se perceber se o que foi detetado é um UAS, e se for, se representa ou não uma ameaça. Se der positivo para UAS inimigo, e depois de o alvo ter sido adquirido, inicia-se a terceira fase, o seguimento do alvo, sendo que vários sensores acompanham o UAV, enquanto a informação sobre ele é disseminada. A fase seguinte é a de neutralização do UAS. Isso pressupõe tanto impedir que o UAS consiga cumprir a sua missão, como a sua destruição física. Por fim, faz-se a análise (se possível) do próprio UAV, com o objetivo de descobrir quem é o seu proprietário e porque foi utilizado, qual a sua trajetória e local de lançamento, bem como obter outras informações a partir das aplicações instaladas no controlo remoto e no dispositivo móvel.

Para cada uma dessas fases, há vários sistemas disponíveis. Dos equipamentos de deteção e seguimento, o radar é dos mais utilizados. Deteta a presença de UAV através da sua assinatura radar e por vezes emprega algoritmos que lhe permitem distinguir entre UAV e outros "alvos", como pássaros. (Michel, 2018). É uma tecnologia muito versátil, capaz de detetar e seguir alvos de vários tamanhos ao longo de vários quilómetros de distância. No entanto, se a RCS do UAV for desconhecida, a identificação pode ser difícil se se usar só o radar (Birch et al., 2015).

Já um equipamento de radiofrequência (RF) deteta UAV através do *scanning* das frequências nas quais a maioria dos UAS costuma operar (Michel, 2018). É um equipamento de deteção relativamente barato e a maioria dos UAS COTS emite sinais facilmente detetáveis. Tem a desvantagem de não conseguir lidar com uma ameaça que não emita sinais rádio (Birch et al., 2015).

Outro sistema de deteção e seguimento, o eletro-ótico, deteta UAV baseando-se na sua assinatura visual (Michel, 2018). Tem um baixo custo por unidade e há muitas opções no mercado. No entanto, é facilmente afetado pelas condições ambientais, requer iluminação à noite, tem baixo contraste e requer uma outra modalidade para um maior volume de pesquisa (Birch et al., 2015).

Um equipamento de infravermelhos deteta UAV através da sua assinatura térmica (Michel, 2018), o que ajuda a reduzir o *clutter* do meio envolvente. Trabalha bem à noite e é menos suscetível às condições atmosféricas. Infelizmente, a maioria dos UAS tem baixa assinatura térmica (Birch et al., 2015).

Os sistemas de deteção magnética detetam UAV através dos seus componentes em metal. No entanto, a maioria dos LSS UAS usa poucas peças metálicas, o que limita a sua utilidade (Birch et al., 2015).

O recurso a observadores humanos é uma boa opção, pois têm uma capacidade de classificação sem paralelo e são capazes de iniciar técnicas de neutralização. Porém, o seu rendimento baixa quando estão em longa e constante monotorização e têm elevados custos associados.

Os sensores acústicos detetam a ameaça através do som produzido pelos seus motores (Michel, 2018). São baratos e atuam de forma passiva. As suas desvantagens são a necessidade de uma base de dados de assinaturas acústicas conhecidas, o desconhecimento do alcance máximo, que é afetado pelo vento, e não se consegue prever qual o rácio de alarme num ambiente saturado de ruído, como o urbano (Birch et al., 2015).

Todos os sistemas acima descritos têm as suas vantagens e desvantagens, não havendo um cem por cento eficaz. Assim, devem ser utilizados em conjunto, de modo a aumentar a sua capacidade de deteção, seguimento e identificação do UAV.

Quanto aos sistemas de neutralização, estes tanto podem ser desenhados para impedir que o UAS cumpra a sua missão, como podem ter como ter objetivo a destruição física do UAV. Equipamentos que façam *jamming* ao sinal de radiofrequência são um bom exemplo do primeiro tipo. Ao aumentarem o ruído ambiente, interrompem o *link* do sinal de controlo entre o UAV e o seu operador, impedindo este de controlar a aeronave. Outro exemplo são os *Jammers* ao *Global Navigation Satellite System* (GNSS). Ao

interferirem com o sinal do GNSS, não permitindo que o UAV o receba, afetam o sistema de navegação do UAV. É também possível fazer *Spoofing* ao sinal de controlo, o que permite que outros assumam o controlo do UAV, sobrepondo-se ao sinal de controlo original (Michel, 2018).

Se a intenção, ou a necessidade, for a de destruir o UAV, podem ser utilizados projéteis, sejam eles munições normais ou específicas para este tipo de alvo, armas laser, que através de energia dirigida desfazem os componentes vitais do UAV, e redes, lançadas de modo a prender o UAV (Michel, 2018).

As aves predatórias, como as águias, embora não sendo propriamente um sistema C-UAS, são ainda assim consideradas como um meio de defesa anti UAS COTS. A polícia holandesa tem vindo a treiná-las para caçarem UAS, obtendo bons resultados e levando forças de segurança de outros países a interessarem-se também por essa ideia (Pultarova, 2016).

CAPÍTULO 5 – Doutrina C-UAS

O desenvolvimento de doutrina C-UAS advém da necessidade de fornecer às forças no terreno a formação e os meios capazes de contrariar a ameaça deste tipo. Várias organizações têm vindo a desenvolver trabalhos e documentos nesse sentido.

A NATO, por considerar que os UAS de pequeno porte são uma ameaça para os países que a constituem e respetivas forças, está a desenvolver esforços para encontrar o melhor modo de os contrariar. No entanto, atualmente, a NATO ainda não tem uma estrutura suficientemente abrangente e capaz de coordenar esses mesmos esforços (NATO Air and Missile Defence Committee, 2018).

Também a Marinha Portuguesa, na Diretiva Estratégica da Marinha de 2018, expressa a sua vontade em desenvolver *capacidades defensivas contra este tipo de sistemas* (UAS). Para o efeito, tem vindo a testar essas mesmas capacidades, como por exemplo no exercício SWORDFISH18, e o Centro Integrado de Treino e Avaliação Naval (CITAN) já desenvolveu um documento sobre a utilização de UAS e maneiras de os neutralizar.

O Exército dos Estados Unidos da América (*United States Army*, US *Army*) tem dedicado especial atenção a este tema, uma vez que já enfrentou esta ameaça no campo de batalha.

Desse modo, neste capítulo são analisadas três publicações do US *Army*:

a) ATP[18] 3-01.81 *Counter-Unmanned Aircraft System Techniques;*
b) ATP 3-01.8 *Techniques for Combined Arms for Air Defense;*
c) *Counter - Unmanned Aircraft System Strategy Extract.*

A intenção é recolher os principais conceitos e técnicas de defesa anti UAS e adotá-los para a especificidade da defesa contra UAS COTS no âmbito da HP.

[18] *Army Techniques Publication*

5.1 Análise do ATP 3-01.81 *Counter-Unmanned Aircraft System Techniques*

O ATP 3-01.81 C-UAS fornece considerações sobre o planeamento da defesa contra LSS UAS durante operações militares e realça desde o início que a defesa contra UAS é uma tarefa difícil e não existe apenas uma só solução para enfrentar todas as categorias da ameaça do tipo LSS (US Army, 2017).

De acordo com essa publicação, LSS UAS engloba os UAS dos Grupos 1, 2 e 3 (classificação do DoD). Os UAS dos Grupos 1 e 2 são os mais difíceis de detetar no campo de batalha e constituem uma das mais significantes ameaças contra as forças amigas no terreno. O planeamento destinado a contrariar essa ameaça deve ter em consideração que as plataformas de UAS possuem várias capacidades, podendo desempenhar diferentes missões (US Army, 2017).

O treino dado aos militares assume um papel relevante. O comandante da força deve adverti-la sobre quais as capacidades da ameaça do tipo LSS UAS, quais os perigos associados e como deve a unidade reagir quando é detetado um UAS. Deve-se treinar constantemente métodos de observação e de relato. Quando detetado um UAS, a unidade deve reagir da maneira mais eficaz naquela situação. Nem sempre a defesa contra UAS passa pela utilização das armas à disposição, podendo a resposta por parte da unidade ser simplesmente dispersar ou procurar abrigo (US Army, 2017). De acordo com o ATP 3-01-81, seguem exemplos de treino a efetuar contra a ameaça LSS UAS:

a) Emprego de observadores dedicados, utilizando técnicas de vigilância aérea;
b) Treino de reconhecimento visual de aeronaves;
c) Treino de técnicas para evitar a ameaça aérea;
d) Estabelecer uma força de segurança e uma força de reação rápida;
e) Estabelecer uma rede de sensores de aviso antecipado;
f) Realizar procedimentos de relato de UAS;
g) Treinar técnicas de camuflagem e de abrigo;
h) Selecionar os meios de defesa contra LSS UAS mais eficazes;
i) Fazer a análise das possíveis ameaças que uma unidade pode ter;
j) Treinar a reconstituição da unidade
k) Disseminar o aviso de ameaça aérea e o estado de controlo das armas.

O ATP 3-01-81 aborda as considerações de planeamento de três escalões: brigada, batalhão e companhia.

A nível de brigada, as principais ações a tomar são, entre outras, as seguintes:

a) Definir os meios a defender, com base na informação recebida, na avaliação do risco e nas avaliações do comandante;
b) Definir as ROE;
c) Disseminar os estados de alerta das armas (que podem ser diferentes para cada tipo de UAS);
d) Estabelecer o nível de controlo;
e) Informar os militares dos critérios C-UAS;
f) Estabelecer avisos de ameaça aérea locais e gerais;
g) Coordenar com as forças amigas a utilização do espaço aéreo, de modo a reduzir ataques fratricidas;
h) Estabelecer procedimentos de notificação.

A nível de batalhão, as condições ambientais são bastante relevantes, devendo por isso o planeamento neste nível incluir as seguintes interrogações:

a) As condições ambientais e meteorológicas afetarão a capacidade do inimigo para realizar ações de reconhecimento, vigilância e recolha de informações sobre as operações das forças amigas, utilizando UAS?
b) Existe algo no terreno que afete o lançamento e a recolha do UAS?
c) Qual é o padrão de atividades associadas à operações de UAS por parte do adversário?
d) Existem infraestruturas civis na área que possam providenciar abrigo e cobertura ao inimigo?
e) O batalhão tem meios capazes de deter o uso de UAS inimigos?
f) Qual é a atual avaliação da ameaça do tipo UAS?

O planeamento de escalão batalhão tem ainda de considerar:

a) A possível ameaça de grupos de UAS a operar na sua área de operações;
b) As capacidades da ameaça do tipo UAS;
c) O nº de UAS espectáveis que realizem ataques na área de operações;
d) As capacidades de *payload*;
e) As capacidades dos UAS de evitar os sistemas radar e de aviso antecipado;
f) Os perfis de voo;
g) A coordenação dos sensores com os centros de comando.

O objetivo das considerações de escalão companhia é garantir que cada militar está devidamente preparado para enfrentar a ameaça do tipo LSS UAS, com especial foco nas suas capacidades de observador do espaço aéreo. O pessoal destacado com esta missão tem de se manter bem vigilante e garantir uma correta cobertura do espaço aéreo. O seu relato de deteção de uma ameaça do tipo UAS deve incluir a estima da localização da ameaça a partir da posição do observador, podendo ser utilizados pontos de referência. Os observadores devem relatar a distância a que o UAS foi detetado, as horas, a duração da deteção, a sua elevação o seu tamanho e qual a direção para onde seguia. Se o UAS detetado for do grupo 1, o observador deve procurar outras possíveis ameaças nas proximidades, como por exemplo forças inimigas ou equipas de operadores de UAS:

Os observadores devem conseguir realizar as suas operações durante quaisquer condições, seja de dia, de noite ou com visibilidade reduzida. Desse modo, têm de estar equipados com o material adequado.

5.2 Análise do ATP 3-01.8 *Techniques for Combined Arms for Air Defense*

O ATP 3-01.8 "*Techniques for Combined Arms for Air Defense"* foca-se no como deve uma força combinada proteger-se de um ataque aéreo inimigo, considerando que a ameaça aérea inclui aeronaves de asa fixa ou rotativa, *rockets*, artilharia, morteiros, mísseis e UAS.

Para uma defesa eficaz, o planeamento assume desde o início um papel fundamental, pois se for o adequado, o comando assegurará que as unidades empregarão as medidas de proteção da força adequadas contra a ameaça UAS. O planeamento a nível tático inclui:

- Incorporação de redes de aviso antecipado
- Identificar as capacidades e os perfis das plataformas de UAS inimigas
- Identificar a localização de possíveis alvos
- Treinar as tropas no terreno para identificar os UAS
- Coordenar ações entre postos de comando e unidades de defesa aérea
- Estabelecer procedimentos de relatos:
    - identificação de UAS
    - aviso posterior para o comando
- Minimizar a exposição das unidades às ameaças dos UAS
- Monitorizar as ações dos UAS e coordenar ações de apoio

A recolha de informação sobre a ameaça é fundamental para ajudar a derrota-la. Assim, deve-se tentar responder às seguintes questões (US Army, 2016a):

- Que tipos de UAS o inimigo tem?
- Como vão ser utilizados (reconhecimento, vigilância, apoio de fogos, aquisição de alvos ou ataque, etc)?
- Que forças são apoiadas por cada um dos UAS?
- Que silhuetas lhes estão associadas?
- Quais são os possíveis pontos de lançamentos dos UAS?
- Quais são os seus alcances e autonomia?
- Como é o histórico de combate do inimigo?
- Quais são as suas características/capacidades?
    - Tamanho
    - Desempenho (velocidade, altitude, restrições de lançamento)
    - Prestação e alcance
    - Fatores limitativos do terreno e contornos de voo
    - Aquisição do alvo e *standoff* range
    - Conjunto de sensores e carga útil (máximo peso, tipo e misturas de carga)
    - Quanto tempo pode o UAS estar a operar
    - Efeitos de visibilidade na adquirição
    - Modos de recolha e tempo de resposta
    - Capacidade em tempo real, de *data-link*
    - Modelos de controlo (controlado no solo ou pré-programado)
    - Experiência dos operadores
    - Armas que transporta

A tarefa de identificar corretamente que tipo de UAS é, é muito difícil, uma vez que estas plataformas têm pouca ou nenhuma identificação, ou IFF. Deve-se designar uma pessoa, ou equipas, para observar e vigiar o horizonte. Há que prestar especial atenção em alturas chave, como imediatamente depois de ataques com fogo indireto, durante ou depois de confrontos importantes ou durante ou depois de *raids*. Os comandantes devem treinar os seus homens para reportarem e se coordenarem eficazmente com os elementos das operações ou informações (de modo a identificarem padrões dos UAS inimigos). As unidades devem requerer e coordenar a informação sobre

ameaça aéreas, e observar todas as técnicas inimigas usadas, de modo a definir Táticas, técnicas e Procedimentos (TTP). O comando deve ser avisado, assim como as outras unidades, sendo recomendado o uso do formato de relatório seguinte:

Line	***Information Example***	***Example***
1	Unit call sign and frequency	Red 1, FHXXX
2	Unit location	6 to 8 digit grid coordinate
3	Location of threat unmanned aircraft system	Grid or distance and direction from reporting unit location
4	Time threat unmanned aircraft system asset spotted/detected	Date/time group (DTG):
5	Estimated time on site	Was threat unmanned aircraft system asset approach observed or was it spotted overhead? How long might it have been there?
6	Flight characteristics	Is threat unmanned aircraft system loitering in one spot (possibly already spotted reporting unit), is it flying straight (en route to loitering location), what is the direction of flight, or is it flying randomly (searching)?
7	Estimated size, elevation, and physical description	Wingspan, height, color, tail configuration, other distinguish markings.

Figura 8- Exemplo de formato de relatório. Fonte: (US Army, 2016a)

Para neutralizar a ameaça não é obrigatório destruí-la, embora exista essa opção. Soluções para anular a ameaça podem passar por limitar a vigilância e recolha de informações por parte dos UAS ou seguir o UAS até ao seu operador. Pode haver pouco tempo para atacar UAS inimigos, devido à sua velocidade e altitude. Controladores do espaço aéreo podem encontrar dificuldades semelhantes devido a:

- Capacidades dos sensores utilizados nas redes de aviso antecipado;
- Pequena RCS de muitos dos UAS;
- Congestão do espaço aéreo.

Para atacar um UAS, é também importante descobrir e neutralizar o seu ponto de lançamento e respetivo operador.

5.3 Análise do *Counter - Unmanned Aircraft System Strategy Extract*

No documento "*Counter - Unmanned Aircraft System Strategy Extract*", de 5 de outubro de 2016, são propostas quatro linhas de ação principais: *Mission Command*, *Detection*, *Identification* e *Defeat*.

Mission Command, que abrange as outras três, fazendo-as atuar de forma integrada e coordenada, de modo a aumentar a sua eficácia, subdivide-se em três capacidades. A primeira é o controlo e gestão do espaço aéreo, por forma a assegurar o

apoio e controlo de aeronaves tripuladas e não tripuladas e a correta identificação de alvos de qualquer tipo, e autorizar ataques no espaço aéreo. A segunda refere-se a ROE e controlo de risco, pois ter regras de empenhamento para este tipo de situações/ameaça é fundamental para garantir uma resposta correta e atempada. Por fim, o panorama tático aéreo e aviso antecipado, uma vez que todas as medidas C-UAS são mais eficazes quando os seus sistemas e operadores estão preparados para atuar desde o primeiro momento; quanto maior for a quantidade e a qualidade do aviso antecipado e da compilação tática aérea, mais eficaz será a resposta à ameaça.

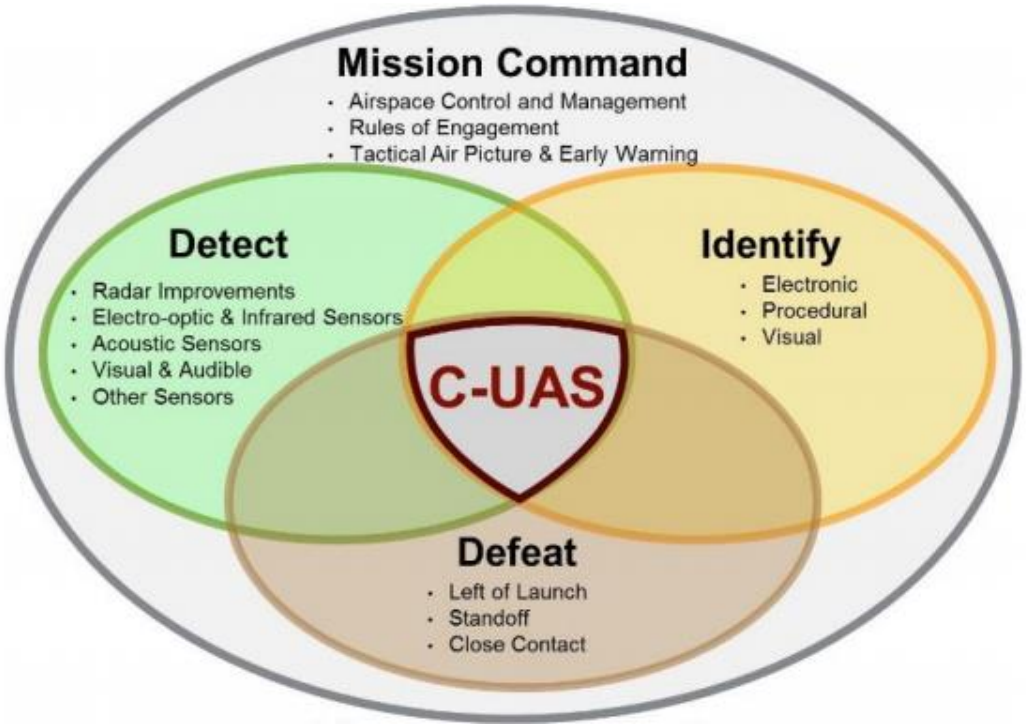


Figura 9 - Principais linhas de ação. Fonte: (US Army, 2016a)

Detection engloba todos os sistemas e iniciativas que contribuem para detetar UAS, transmitindo essa informação para os elementos responsáveis. Há que ter em conta que há UAS com baixas RCS, pequenas assinaturas IR e pegadas eletromagnéticas limitadas, sendo por isso necessário que os sensores C-UAS evoluam, por forma a aumentar as suas capacidades. *Detection* subdivide-se em cinco tipos de deteção: radar, sensores EO/IR, outros sensores eletromagnéticos e sensores eletrónicos, sensores acústicos e visual e auditiva.

Identification é a capacidade de, depois de detetado o objeto, o conseguir classificar como ameaça, amigo ou neutral. Uma correta identificação permite evitar o risco de atingir forças amigas e garante uma atempada e adequada implementação de

ROE. Os meios eletrónicos são, por norma, os mais rápidos e fiáveis. Há sensores que já conseguem classificar os UAV baseando-se na sua *radar cross section*, assinaturas de infravermelhos ou outras assinaturas eletrónicas. Recorre-se também à observação de procedimentos, ou seja, análise de comportamentos próprios que permitam atribuir a correta classificação. A identificação visual desempenha um papel importante, pois embora exista uma grande variedade de tipos de UAS, eles assentam em formas físicas básicas. Os militares devem estar treinados para efetuar uma correta identificação, baseando-se em determinadas características (asa fixa vs asa rotativa, por exemplo).

Defeat reúne todos os equipamentos capazes de derrotar um UAS. A estratégia proposta é a da "defesa em profundidade", ou por "camadas", caraterizando três fases distintas: *left-of-launch*, *standoff* e *close contact*. Estas fases de neutralização do UAS estão ordenadas da mais preferencial (ainda antes de descolar) para a menos (em contacto próximo).

- *Left-of-launch* envolve todas as tentativas efetuadas para impedir que os UAV possam sequer serem utilizados e engloba a prevenção da proliferação (recorrendo à política e diplomacia para evitar que certos países ou grupos não-estatais, considerados como possível ameaça, não consigam ter acesso a estas tecnologias), a facilidade de ataque (a instalações responsáveis pelo lançamento, manutenção e comando e controlo de UAS) e as operações de guerra eletrónica e do ciberespaço (uma vez que muitos dos UAS comerciais dependem destes meios para operar).

- *Standoff* refere-se às operações/ataques cujo objetivo é o de neutralizar as operações envolvendo UAS, ainda antes de conseguirem empregar as suas capacidades. Atacar os operadores de UAS ou os locais de onde operam; utilizar energia eletromagnética para controlar o espectro eletromagnético e/ou atacar o inimigo (*Offensive Electronic Attack*); recorrer a uma contra-vigilância/reconhecimento eficaz, por forma a que os UAS não possam realizar operações de vigilância/reconhecimento; e utilizar sistemas de armas de defesa aérea.

- *Close contact* ocorre quando não se conseguiu neutralizar os UAS nas duas fases anteriores. A tarefa de neutralizar a ameaça vai recair sobre as unidades que os UAS consideraram como alvo. Assim, é necessário que cada combatente esteja devidamente treinado, para saber como agir; uma vez que a principal função dos UAS é detetar e identificar alvos, se lhes retirarmos essa capacidade deixam de surtir efeito, logo

camuflagem ou fumo podem ser suficientes para anular essa ameaça; em última instância, deve-se fazer uso de armas antiaéreas ou ligeiras.

CAPÍTULO 6 – A defesa contra UAS COTS no âmbito da HP

Neste capítulo são apresentadas propostas a adotar no âmbito da HP, de modo a se conseguir contrariar uma ameaça do tipo UAS COTS.

6.1 Táticas de utilização de UAS COTS contra HPO

De acordo com o ATP-94, durante a fase de planeamento deve-se definir a ameaça, o que engloba perceber quem é a ameaça, quais os seus alvos, quais os seus objetivos, que táticas serão utilizadas e que respostas a essa ameaça devem ser aplicadas. O emprego de UAS COTS é um exemplo de táticas passíveis de adotar, sendo que existem várias formas de utilização de UAS COTS (Tabela 4).

A Tabela 4 foi elabora com base nas conclusões obtidas no capítulo 3, onde se tomou em consideração as caraterísticas dos UAS COTS, os seus pontos fortes/fracos e casos da sua utilização em ações de combate/ilegais.

A cada tipo de táticas foram associados três parâmetros, seguindo o modelo descrito no ATP-74: táticas, considerações para contrariar a ameaça e principais fatores de planeamento.

O primeiro parâmetro descreve como são empregues os UAS COTS e quais os seus objetivos. O segundo parâmetro sugere como se pode contraria essa ameaça, evitando que o UAS seja utilizado ou neutralizando-o. O último parâmetro aborda quais os fatores de planeamento a considerar.

TÁTICAS DE UTILIZAÇÃO DE UAS COTS CONTRA HPO		
TIPO	COMO	EXEMPLO
Vigilância e recolha de informação.	Recorre ao sensor de imagem que o UAV transporta.	O UAV descola de um ponto afastado dos limites do porto e recolhe imagens dos navios atracados e das instalações portuárias.
Guerra eletrónica.	Transporte de um *jammer* ou de um *spoofer*.	O UAV é utilizado para empastelar sensores distribuídos ao longo do porto.
Ataques cinéticos.	Transportando explosivos ou outro tipo de arma.	O UAV tem um dispositivo que lhe permite largar a carga do tipo IED sobre o alvo, ou o UAV é utilizado como um "*kamikaze*".
Interferência no espaço aéreo.	O UAV é orientado até ao local onde decorrem operações de aterragem/ descolagem de uma aeronave.	O UAV é guiado contra as hélices de um helicóptero que está a participar numa evacuação médica dentro do perímetro do porto.
Transporte de material ilegal ou roubado.	O UAV é utilizado para inserir ou retirar material de dentro dos limites do porto	O UAV é utilizado para transportar um IED e colocá-lo num sítio específico, onde outro elemento da força o irá buscar e utilizar.
Coordenação de ataques (C2).	Usando sensores eletro-óticos para ter imagens em tempo real do ataque em curso.	Um grupo terrorista infiltrado dentro do perímetro do porto é orientado pelo seu líder, que se encontra no exterior a receber imagens aéreas da zona, provenientes do UAV.
"Ataque" não planeado.	Descuido do operador ou algum problema nos vários elementos que compõe um UAS.	Um operador amador perdeu o controlo da aeronave, levando esta a despenhar-se dentro dos limites do porto, sobre uma viatura.
Ataque de enxame (saturação).	São utilizados vários UAS ao mesmo tempo, sobre a mesma área.	Ataque multi-eixo, com diferentes UAS a cumprir diferentes missões, com a intenção de saturar as defesas adversárias.

Tabela 4 - Tipos e exemplos de táticas contra HPO utilizando UAS COTS.

As medidas C-UAS têm de lidar com o reduzido tempo de reação disponível para enfrentar a ameaça de um só UAS, e o número de meios disponíveis para neutralizar um enxame de vários UAS (Warnke, n.d.).

6.1.1 Vigilância e recolha de informação.

1. Táticas: As ações de vigilância e recolha de informação com recurso a UAS COTS têm como principal objetivo auxiliar no planeamento de ataques (US Army, 2016a). Não existe uma ameaça direta, por parte dos UAS COTS, contra as forças e unidades amigas. Por norma, os UAS que executam este tipo de missão não se aproximam muito dos seus alvos.

2. Considerações para contrariar o ataque: Neste tipo de ações, a câmara embarcada no UAS COTS constitui a principal preocupação a ter em conta pelas forças e unidades amigas. Tudo o que for negar a capacidade de recolha de imagens, ou a sua correta análise, deve ser aplicado. Redes de camuflagem dispostas ao longo das unidades navais e instalações portuárias, de modo a cobrir equipamentos ou armas, são uma boa opção. Pode também ser utilizado fumo, se a situação operacional o permitir. Se possível, retirar símbolos identificadores, como por exemplo as passadeiras dos elementos que se encontrem no exterior do navio ou placas de identificação das instalações. Caso existam, equipamentos de *jamming* ou *spoofing* são uma boa opção, se o respetivo alcance for o suficiente (ver Apêndice A). Pode ser necessário prepararem-se medidas para abater o UAS.

3. Principais fatores de planeamento: Deve-se minimizar a exposição de elementos ao UAS. Assim, todos os militares que não sejam necessários no exterior do navio devem recolher ao seu interior.

6.1.2 Guerra eletrónica.

1. Táticas: O UAS COTS transporta um equipamento de *jamming* ou *spoofing* e tenta empastelar sistemas de comunicações, como redes de telemóvel e outras redes sem fios, e sensores, como o GPS e radares.

2. Considerações para contrariar o ataque**:** Eliminar a fonte emissora ou utilizar medidas de proteção eletrónica (*Electronic Protective Measures*, EPM).

3. Principais fatores de planeamento: Quando um dos sistemas que depende da utilização do espectro eletromagnético sofre falhas, umas das possíveis causas pode ser um ataque eletrónico. Os operadores dos sistemas afetados devem ter formação adequada para reagirem adequadamente a este ataque.

6.1.3 Ataques cinéticos.

1. Táticas: Dentro do grupo de ataques cinéticos incluem-se os do tipo "kamikaze", onde o próprio UAS é utilizado como arma, estando por norma armadilhado com explosivos, e os de lançamento de munições, como granadas ou IED. O UAS pode ainda transportar WMD e armas de guerra CBRN. O objetivo deste tipo de ataques é o de destruir equipamento vital (antenas de comunicação ou radares, por exemplo), eliminar um alvo específico (como o comandante de um navio), incapacitar meios (por exemplo, o HPM) e provocar baixas nas forças amigas (Wallace & Loffi, 2015).

2. Considerações para contrariar o ataque: Neste tipo de utilização de UAS COTS, é imperativo que se recorra de imediato à tentativa da sua destruição, ou pelo menos tentar afastar o UAS do seu alvo. Jatos de água, armamento convencional ou redes podem ser opções à disposição dos militares embarcados nos navios. Também nestes casos, o recurso a um equipamento de *jamming* ou de *spoofing* pode ter um resultado favorável, pois permite neutralizar a tentativa de ataque (ver Apêndice A).

3. Principais fatores de planeamento**:** Embora a utilização de armamento portátil convencional para abater um UAS seja uma sugestão a ter em conta, há que considerar a hipótese de que uma munição acertar num UAS carregado de material explosivo ou CBRN possa provocar consequências bem piores das que se estão a tentar evitar. Assim, deve-se considerar que a utilização de redes, jatos de água ou equipamentos de *jamming/spoofing* são mais seguros, devendo ser dada primazia a estes métodos. É também recomendado que todos os militares que estejam no exterior dos navios, mas que não estejam envolvidos em atividades fundamentais, recolham para os interiores.

6.1.4 Interferência no espaço aéreo.

1. Táticas: Os UAS COTS são usados para sobrevoar zonas onde operam outras aeronaves, com o objetivo de as danificar, ou pelo menos evitar que estas cumpram as suas missões (Wallace & Loffi, 2015).

2. Considerações para contrariar o ataque: Neste caso o mais importante é a capacidade de aviso antecipado, sendo os sistemas de vigilância e de deteção fundamentais. Mal se detete um UAS COTS nas imediações da aeronave amiga, esta deve de ser imediatamente informada e afastada do local, se tal for possível.

3. Principais fatores de planeamento: Garantir uma EZ dedicada para as áreas de operações de voo.

6.1.5 Transporte de material ilegal ou roubado.

1. Táticas: Os UAS COTS podem ser utilizados para transportar material para dentro da área do porto, como por exemplo, equipamento que possa ser utilizado num ataque. Do mesmo modo, o UAS COTS pode ser usado levar material para o exterior, tal como documentos classificados roubado (Wallace & Loffi, 2015).

2. Considerações para contrariar o ataque: A existência de uma boa rede de sensores ajuda a minimizar as hipóteses de sucesso de inserir ou retirar algo da área do porto. Patrulhas constantes do perímetro também contribuem para a eficácia da neutralização deste tipo de ações

3. Principais fatores de planeamento: Se o UAS COTS é usado para colocar ou retirar algo das zonas do porto, tal revela que existe alguém que recebe ou envia o material. Os serviços de contrainformação devem ser dotados de meios que lhes permitam detetar e vigiar elementos suspeitos que tenham acesso às áreas portuárias.

6.1.6 Coordenação de ataques (C2).

1. Táticas: Os UAS são operados de modo a transmitirem, em tempo real, informação para os líderes do ataque. Normalmente existe uma força inimiga no terreno, que vai recebendo ordens dos seus líderes sobre para onde se movimentar e que ameaças tem nas suas imediações (Rassler, 2018).

2. Considerações para contrariar o ataque: Sistemas de *jamming* podem impedir que os UAS se aproximem o suficiente para recolher informação útil (ver Apêndice A). Por norma, neste caso os UAS acompanham as forças inimigas, o que pode dar às forças amigas a sua localização. O recurso ao armamento ligeiro pode ser o suficiente para neutralizar esta ameaça

3. Principais fatores de planeamento: Também neste caso, não existe uma ameaça direta, por parte dos UAS COTS, contra as forças e unidades amigas. Estes têm de ter em consideração que se forem vistos pelas câmaras do UAS, isso quer dizer que o inimigo também sabe onde eles se encontram. Se possível, devem dispersar ou recorrer a técnicas que impeçam o inimigo de ter uma boa imagem sobre a situação no terreno.

6.1.7 "Ataque" não planeado.

1. Táticas: Um operador amador, sem experiência, perde o controlo do UAS COTS e este provoca um acidente dentro do perímetro do porto (Wallace & Loffi, 2015)

2. Considerações para contrariar o ataque: Garantir que existe uma zona de proibição de voo de UAS COTS sobre os portos e criar uma EZ suficientemente capaz de manter civis a uma distância que caso estes operem UAS COTS, não consigam alcançar a área dos portos.

3. Principais fatores de planeamento: Esta é uma situação peculiar, pois qualquer dano causado foi por acidente. O HPC pode aproveitar estes casos para perceber como é que o UAS invadiu o perímetro do porto, com a intenção de melhorar as suas defesas.

6.1.8 Ataque de enxame (saturação).

1. Táticas: Vários UAS COTS, de vários tipos e a desempenhar diferentes missões são utilizados ao mesmo tempo, com o objetivo de saturar as defesas (US Army, 2016a).

2. Considerações para contrariar o ataque: Este é o tipo de ataque mais perigoso e mais difícil de contrariar. Neste caso, o acesso antecipado a informações sobre a possibilidade da ocorrência do ataque é fundamental para a eficácia da sua neutralização.

3. Principais fatores de planeamento: Um grande número de UAS COTS a operar na mesma zona pode simbolizar a presença de uma grande força de operadores nas imediações. Caso o HPC considere seguro, a ação de patrulhas no exterior pode ajudar a minimizar os efeitos do ataque.

6.2 Casos particulares

6.2.1 Vigilância e aviso antecipado

Os ataques levados a cabo por UAS COTS caracterizam-se por serem rápidos e difíceis de detetar. A existência de uma rede de sensores capazes de detetar, identificar e seguir um UAS COTS contribui para aumentar o tempo de reação do HPC e das suas unidades, o que permitirá que estas adotem os melhores métodos de defesa.

Deve ser feito um esforço no sentido de treinar os elementos responsáveis pela vigilância e patrulha das áreas portuárias na capacidade de reconhecimento visual dos tipos de UAS COTS e nos procedimentos de relato.

Para ajudar no reconhecimento das aeronaves, deve ser dado, sempre que se considerar necessário, um briefing sobre os tipos de UAS passíveis de serem utilizados pelo inimigo, as suas caraterísticas, e o tipo de ataques que podem executar. Todos os elementos devem conhecer a ameaça e ser capazes de a identificar.

Quem avistar o UAS deve preocupar-se por comunicar tal facto ao comando, sendo este responsável por disseminar a informação e preparar as medidas a adotar. O relato do avistamento do UAS tem de ser o mais completo possível, sendo apresentado o seguinte exemplo:

A) Localização
B) De onde vem
C) Descrição física (se é de asa fixa ou rotativa, marcas características)
D) Altitude a que opera
E) Velocidade
F) Que tipo de carga tem (se tem câmara, se transporta algum objeto)
G) Perfis de voo (se é estacionário, se faz constantes passagens)
H) Qual o modelo

Realça-se o ponto H), onde a capacidade de quem detetou o UAS o saber identificar corretamente assume bastante importância.

6.2.2 *Rules of Engagement*

Uma vez que a aeronave é não é tripulada, as ROE podem ser mais permissivas do que seriam caso a ameaça fosse uma aeronave tripulada. Se o HPC tiver de requerer

ROE, deve destacar esse facto. Pode também acrescentar que devido à furtividade dos UAS COTS, estes podem ser detetados já muito tarde, reduzindo o tempo de reação das unidades atribuídas ao HPC. Por isso, as ROE devem estar delegadas nos escalões mais baixos, com a intenção de permitir uma rápida intervenção.

6.2.3 Contramedidas Passivas

Inclui sistemas de aviso antecipado e sistemas de *Electronic Countermeasures* (ECM) (Dudush et al., 2018).

6.2.4 Contramedidas Ativas

De acordo com o ATP-94, de modo a contrariar as ameaças aéreas assimétricas que podem ocorrer durante uma HPO, o HPC deve utilizar as unidades de *Surface-Based Air Defence* (SBAD) de que dispõe para defender as suas forças e infraestruturas críticas dentro da HP TAOR (NATO, 2017b). Os sistemas SBAD permitem destruir a aeronave, degradar a sua habilidade para voar ou evitar que o UAV cumpra a sua missão. Como efeito secundário, também reduzem as capacidades do *payload* transportado ou inutiliza-o completamente (JAPCC, 2014).

No entanto, como descrito ao longo desta dissertação, os UAS COTS têm características que lhes permitem evitar os sistemas convencionais de defesa antiaérea, obrigando à adoção de sistemas C-UAS próprios para UAS COTS.

6.2.5 *Host Nation*

A relação com a nação onde se encontra o porto ganha um novo e importante significado quando se aborda a defesa anti UAS COTS. As autoridades locais podem ajudar a estabelecer uma EZ perto do porto, que afaste os operadores de UAS para áreas onde não conseguem alcançar os limites do porto. As autoridades locais conseguem também ajudar a controlar a importação e a venda de UAS COTS nesse país, reduzindo a facilidade com que certos grupos (potenciais ameaças) os adquirem.

6.2.6 Sugestão de modelo a adotar por Unidades Navais nacionais em Condição Geral 5 – Navio atracado na BNL

O modelo abaixo descrito é uma sugestão para ser adotada pelos navios da MP quando em Condição Geral 5 – Navio atracado na BNL, e é avistado um UAS nas suas

imediações. A necessidade de criação deste modelo surge das conclusões retiradas do teste realizado na BNL, onde se simulou um ataque a navios por parte de UAS COTS.

Qualquer elemento da guarnição deve, assim que avista um UAV a voar nas imediações do seu navio, informar o ODN.

As seguintes medidas deverão ser executadas:

Oficial de Dia

- Contacta o Oficial de Dia à BNL e confirma se o voo do UAV está autorizado;
- Efetua aviso ao ETO a informar do voo do UAV e ressalva a importância de a guarnição manter uma postura profissional e cuidada.

Sargento de Dia

- Comunica com os navios atracados nos cais mais próximos e informa-os do voo do UAV.

Oficial de Marinheiros/Cabo de Quarto

- Mantem contacto visual com o UAV, de modo a nunca perder a sua posição;
- Efetua registo do UAV (fotografia e vídeo).

Caso se suspeite de que o UAV transporta algum engenho explosivo, ou outro tipo de armamento, deve ser efetuado o seguinte aviso ao ETO:

UAV SUSPEITO A BB/EB/AV/AR/A SOBREVOAR O NAVIO. TODA A GUARNIÇÃO RECOLHE AO INTERIOR.

Oficial de Dia

- Manda estabelecer a Cidadela (nem todos os navios dispõe desta opção);
- Avalia a necessidade de estabelecer uma condição de estanqueidade mais restritiva;
- Manda colocar as mangueiras em carga no exterior do navio (ação a ser efetuada por elementos do grupo de serviço);
- Informa o Oficial de Dia à BNL, o Centro de Operações Marítimas (COMAR) e o Comandante do Navio, caso este não se encontre a bordo;
- Providencia armamento do tipo G3 aos plantões. A ordem de disparo só é dada em caso de confirmação com cem por cento de certeza de que o UAV é mesmo uma ameaça real.

Sargento de Dia

- Garante que a ordem para a guarnição recolher ao interior foi cumprida.

Oficial de Marinheiros/Cabo de Quarto

- Mantem contacto visual com o UAV, de modo a nunca perder a sua posição;
- Efetua registo do UAV (fotografia e vídeo)

CAPÍTULO 7 - Conclusão

Apresentam-se neste capítulo as respostas às Questões Central e Derivadas, elaboradas no início da dissertação e que foram obtidas com o desenvolvimento dos capítulos expostos neste trabalho. Devido à pertinência deste tema, no final deste capítulo sugerem-se três ideias para trabalhos futuros.

7.1 Respostas à Questão Principal e Derivadas

A primeira QD, "Como se materializa a ameaça do tipo UAS COTS?", tinha como objetivo compreender as capacidades e limitações da utilização de UAS COTS em ações ofensivas e perceber como poderiam ser empregues nessas mesmas ações.

Verificou-se que as vantagens que estes sistemas apresentam torna-os aliciantes para forças terroristas e outras não governamentais, existindo já casos da sua utilização por parte desses grupos. Com base nas suas capacidades e no seu histórico de utilização, estipulou-se de que modo poderiam ser empregues, especificamente durante uma ação contra um porto.

Quanto à QD nº 2, "Como funcionam os sistemas C-UAS COTS?", que visava perceber como atuam estes sistemas de modo a neutralizar a ameaça do tipo UAS COTS, concluiu-se que as características dos UAS COTS obrigaram ao desenvolvimento de sistemas específicos para os enfrentar. Os sistemas C-UAS COTS atuam nas áreas da deteção, identificação, seguimento e neutralização, recorrendo a diversos equipamentos como por exemplo radares e *jammers*.

Não existe um sistema que só por si seja suficientemente eficaz e por isso deve-se investir em sistemas completos, com várias capacidades.

A terceira QD, "Que doutrina C-UAS já existe e como pode ser adaptada para o caso específico dos UAS COTS?", respondeu-se principalmente com a análise de duas publicações do Exército Americano, tendo-se também abordado outros documentos.

Por último, apresenta-se a resposta à QC, "Que doutrina deve ser elaborada para se melhor enfrentar a ameaça do tipo UAS COTS, no âmbito da HP?".

Para melhor se enfrentar esta ameaça, há que ter em consideração que existem oito tipo de ataques com recurso a UAS COTS.

7.2 Sugestões para trabalho futuro

A defesa contra UAS no geral, e UAS COTS no particular, é ainda um tema recente, sendo expectável que a ameaça do tipo UAS, comercial ou não, não só continue presente, como até que evolua. É, pois, necessário que se continue a abordar esta temática, motivo pelo qual são apresentadas as seguintes sugestões para trabalho futuro:

a) Desenvolvimento de um sistema específico para a defesa anti UAS COTS, que possa ser empregue a bordo de uma Unidade Naval. Esse sistema deve de ser prático, fácil de transportar e operar.
b) Desenvolvimento de um sistema integrado de deteção e identificação de UAS COTS que possa ser implementado na Base Naval de Lisboa. Tal sistema deve ser constituído por diferentes tipo de sensores, como por exemplo radares e câmaras de infravermelhos, deve compilar a informação recebida sobre a aeronave detetada e apresentar sugestões de ações a tomar contra a mesma.
c) Análise da capacidade de defesa anti UAS COTS do principal porto comercial de Portugal. Devem ser estudados de que modo os UAS COTS seriam empregues, que danos poderiam provocar e quais as suas consequências. Por fim, deve ser elaborado um plano de defesa contra UAS COTS que possa ser implementado nesse porto.

Referências

Agência Lusa. (2018). Drone fechou aeroporto de Lisboa durante dez minutos e desviou dois voos. *Observador*. Retrieved from https://observador.pt/2018/09/20/drone-fechou-aeroporto-de-lisboa-por-dez-minutos-e-desviou-dois-voos/

Alami, M. (2017). Analysis: Hezbollah enters drone age with bombing raids in Syria. Retrieved December 2, 2018, from https://www.middleeasteye.net/news/analysis-hezbollah-enters-drone-age-bombing-raids-syria

Amazon. (2018a). Custo Phantom 4. Retrieved December 4, 2018, from https://www.amazon.com/DJI-Phantom-Starter-Bundle-Controller/dp/B01M06R21I/ref=sr_1_3?ie=UTF8&qid=1543892974&sr=8-3&keywords=drone+phantom+4

Amazon. (2018b). Resultados de procura para "Drone." Retrieved December 4, 2018, from https://www.amazon.com/s/ref=nb_sb_noss_2?url=search-alias%3Daps&field-keywords=drone

Antunes, R. (2018, August). Drones já são muitos e são para todo o serviço. *Visão*. Retrieved from http://visao.sapo.pt/actualidade/sociedade/2018-08-11-Drones-ja-sao-muitos-e-sao-para-todo-o-servico

Arnold, T. D., & Fiore, N. (2019). Five Operational Lessons from the Battle for Mosul. *Military Review*. Retrieved from https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Jan-Feb-2019/Arnold-Mosul/

Birch, G. C., Griffin, J. C., & Erdman, M. K. (2015). UAS Detection , Classification , and Neutralization : Market Survey 2015.

Bliss, D. (2019). Assassinos de Drones: A Nova Guerra dos Céus. Retrieved from https://www.natgeo.pt/ciencia/2019/06/assassinos-de-drones-nova-guerra-dos-ceus

Blom, J. D. (2010). Unmanned Aerial Systems: A Historical Perspective.

Bunker, R. J. (2015). *Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potencials, and Military Implications*.

Buric, M., & Cubber, G. De. (2017). Counter Remotely Piloted Aircraft Systems.

Delgado, J. A. M. (2018). El uso de drones comerciales como vectores terroristas.

DJI. (2018). Active Track. Retrieved December 4, 2018, from https://store.dji.com/guides/film-like-a-pro-with-activetrack/

Dudush, A., Tyutyunnik, V., Trofymov, I., Bortnovs'kiy, S., & Bondarenko, S. (2018). State of the Art and Problems of Defeat of Low, Slow and Small Unmanned Aerial Vehicles. https://doi.org/10.3849/aimt.01233

Ebay. (2018). Resultados para procura de "Drone." Retrieved December 4, 2018, from https://www.ebay.com/sch/i.html?_from=R40&_trksid=m570.l1313&_nkw=drone&_sacat=0

Escorrega, L. C. F. (2009). A Segurança e os " Novos " Riscos e Ameaças : Perspectivas Várias, 1–29.

Exército Português. (2016). PDE 3-37-00 - Tática de Artilharia Antiaérea.

Garcia, L. (2015). *A Contenção da Ameaça UAS*.

Gettinger, D. (2016). *Drones Operating in Syria and Iraq*.

Gusterson, H. (2017). *Drones*. (Antígona, Ed.) (1ª Edição).

Joint Air Power Competence Centre. (2010). Strategic Concept of Employment for Unmanned Aircraft Systems in NATO.

Joint Air Power Competence Centre. (2014). Remotely Piloted Aircraft Systems in Contested Environments. A Vulnerability Analysis.

Jornal de Notícias. (2019). Governo aprova regulamentação de uso de drones. *Jornal de Notícias*. Retrieved from https://www.jn.pt/nacional/interior/governo-aprova-regulamentacao-de-uso-de-drones-10391745.html?utm_source=Push&utm_medium=App&fbclid=IwAR1aZLjQIJMhQ5tuSfm0nft7C6UGjISlaZUgkj9uxLw5K7ll_0ig90CvlMY

Kelly, E. (2018). Venezuela drone attack: Here's what happened with Nicolas Maduro. *USA TODAY*. Retrieved from https://eu.usatoday.com/story/news/politics/2018/08/06/venezuela-drone-attack-nicolas-maduro-assassination-attempt-what-happened/913096002/

Marinha Portuguesa. (2018). Diretiva Estratégica da Marinha 2018.

Marques, M. R. M. (2018). *Reference Model for Interoperability of Autonomous Systems*.

Michel, A. H. (2018). Counter-Drone Systems. Center for the Study of the Drone.

NATO. (2016). AXP-05 Edição C Versão 15 Experimental Tactics and Amplying Tactical Instructions.

NATO. (2017a). ATP-74 (A) Versão 2.

NATO. (2017b). ATP-94 (A) Versão 1 Harbour Protection.

NATO. (2018). AAP-06 NATO Glossary of terms and definitions (English and French).

NATO Air and Missile Defence Committee. (2018). Countering Class I Unmanned Aerial Systems - Practical Framework Outline.

NATO Communications and Information Agency (NCIA). (2018). Notification of Intente to Invite Bids: Provide Counter-Small Unmanned Aircraft Systems (C-SUAS) Capability.

Observador. (2019). Presos recebem contrabando por drone. *Observador*. Retrieved from https://observador.pt/2019/02/27/presos-recebem-contrabando-por-drones/

Oliveira, F. de. (2016). *Unmanned Aerial Systems (UAS): Questões Legais e Éticas da sua utilização no combate ao terrorismo Unmanned Aerial Systems (UAS): Questões Legais e Éticas da sua utilização no combate ao terrorismo*.

Parrot. (2018). Follow me. Retrieved December 4, 2018, from

https://www.parrot.com/global/follow-me

Pomerleau, M. (2017). The elaborate system behind ISIS' drone program. Retrieved December 2, 2018, from https://www.c4isrnet.com/unmanned/uas/2017/01/31/the-elaborate-system-behind-isis-drone-program/

Pultarova, T. (2016). Drone-killing eagles in Holland inspire Metropolitan police. *Engineering and Technology*. Retrieved from https://eandt.theiet.org/content/articles/2016/02/drone-killing-eagles-in-holland-inspire-metropolitan-police/

Rassler, D. (2018). The Islamic State and drones.

Regimento de Artilharia Antiaérea Nº 1. (2017). Informação para a edificação da capacidade de derrube de plataformas aéreas de baixo porte.

Udemy. (2018). Cursos de drone. Retrieved December 4, 2018, from https://www.udemy.com/topic/drone/

US Army. (2016a). ATP 3-01.8 Techniques for Combined Arms for Air Defense.

US Army. (2016b). Counter-Unmanned Aircraft System (C-UAS) Strategy Extract.

US Army. (2017). ATP 3-01.81 Counter-Unmanned Aircraft System Techniques.

Wallace, R. J., & Loffi, J. M. (2015). Examining Unmanned Aerial System Threats & Defenses: A Conceptual Analysis.

Walsh, N. P., Gallón, N., Perez, E., Castrillon, D., Arvanitidis, B., & Hu, C. (2019). Inside the August plot to kill Maduro with drones. *CNN*. Retrieved from https://edition.cnn.com/2019/03/14/americas/venezuela-drone-maduro-intl/index.html

Walters, D. (2016). Countering the Emerging Small UAS Threat: The case for a Coherent Canadian Counter-SUAS Strategy.

Warnke, H. (n.d.). Reconnaissance of LSS-UAS with Focus on EO-Sensors.

Youtube. (2018a). Resultados de procura para "How to fly a drone for beginners." Retrieved December 4, 2018, from https://www.youtube.com/results?search_query=how+to+fly+a+drone+for+beginners+

Youtube. (2018b). Resultados de procura por "How to build a drone."

Apêndices

Apêndice A – Relatório Técnico do Exercício com UAS comerciais na Base Naval de Lisboa, a 12 de fevereiro de 2019

Título:	Utilização de UAV COTS para ataques e defesa contra os mesmos, executado no dia 12 de fevereiro de 2019
Autores:	ASPOF Hipólito Lopes, ASPOF Rodrigues Marante, ASPOF Costa Teles, CTEN EN-AEL Monteiro Marques, CTEN M Nunes dos Santos, CTEN FZ Pereira da Silva, Prof. Sousa Lobo.
Sumário:	Este relatório descreve os testes efetuados no dia Fevereiro de 2019, na Base Naval de Lisboa (BNL), visando verificar as capacidades de ataque por parte de UAV comerciais a navios atracados na BNL, e as capacidades destes para neutralizarem essa ameaça. Os testes foram efetuados no âmbito do projeto CAMELOT e para apoio às dissertações de mestrado dos três aspirantes, coautores deste relatório. Para esses testes, foram utilizados dois UAV COTS, o Bebop2 e o Disco, ambos da marca Parrot e com capacidade *First Person View* (FPV). Os navios alvo do ataque foram a Fragata NRP *Vasco da Gama* e a Corveta NRP *António Enes*. Os oficiais desses navios estavam cientes que o ataque iria ocorrer, bem como o oficial de Dia à BNL, mas a restante guarnição não. O ataque foi realizado por um aspirante localizado na extremidade da BNL, tendo efetuado sucessivas passagens sobre os navios. As guarnições dos navios detetaram os UAV muito tarde, e não foram capazes de manter o contacto com os mesmos, embora tenham cumprido com os procedimentos estipulados. Os atacantes conseguiram obter imagens com grande detalhe dos navios e instalações. Quando o sistema de *jamming* anti-UAV foi acionado, o operador do UAV atacante perdeu imediatamente a ligação, e a ameaça foi neutralizada.
Data:	23/8/2019
Ref:	CINAV-001/2019

1. Enquadramento e motivação para os testes efectuados

A utilização de *Unmanned Aircraft Systems* (UAS) *commercial off the shelf* (COTS) abrange as mais variadas áreas, como a fotografia aérea, a monitorização de culturas agrícolas e a deteção de incêndios, ou simplesmente como hobby. O grande uso por parte do público deve-se, na sua maioria, ao facto de serem baratos, fáceis de adquirir e de operar.

Essas vantagens chamaram também a atenção de grupos terroristas e outras forças não-governamentais que adotaram os UAS COTS e utilizam-nos, por exemplo, em campos de batalha no Iraque e na Síria. Os UAS COTS podem exercer várias funções, como recolha de informação e ataque com recurso a engenhos explosivos.

De modo a aprofundar esse conceito, foram elaboradas três dissertações de mestrado na Escola Naval. Uma delas, "Emprego de veículos aéreos não-tripulados comerciais em operações contra navios e instalações portuárias", visa testar as capacidades dos UAS COTS na realização de ações ofensivas e de apoio a forças de desembarque e propor doutrina para a sua utilização. A segunda, "Defesa contra UAS COTS no âmbito da *Harbour Protection*", tem como objetivo compreender que tipo de ameaça podem os UAS COTS exercer sobre navios atracados, instalações e infraestruturas portuárias e de que modo se deve estruturar a defesa contra essa mesma ameaça. A terceira, "*Development of an Electronic Warfare Packagevisou*" desenvolver um sistema de *jamming* de baixo custo para neutralizar ataques de UAV.

2. Objetivos e material usado nos testes

Para testar as reais capacidades dos UAV em ataques a instalações navais realizou-se um exercício prático, envolvendo UAS COTS e unidades navais, com os seguintes objetivos:

a) Aferir a capacidade de resposta das unidades navais a um possível ataque com recurso a UAS COTS;
b) Verificar se o pessoal está ciente das consequências de um ataque desse tipo;
c) Verificar se o pessoal está preparado para reagir;
d) Verificar se existe uma estrutura de coordenação de resposta ao ataque;
e) Verificar a capacidade de recolha de imagens e a capacidade de manobra de UAS COTS de asa fixa e rotativa;
f) Testar a operação e controlo dos UAS COTS;
g) Verificar o alcance útil e a autonomia dos UAS COTS;

h) Verificar se é possível neutralizar um UAS COTS recorrendo a um *Software Defined Radio* (SDR) de baixo custo, efetuando *jamming* ao sinal de controlo;

O teste foi realizado no dia 12 de fevereiro de 2019, na Base Naval de Lisboa. Os UAS COTS utilizados foram o Parrot Disco FPV (UAV 1), de asa fixa, e o Parrot Bebop 2 FPV (UAV 2), de asa rotativa (Imagem 1 e 2). Os navios que simulavam serem atacados foram os NRP *Vasco da Gama* e NRP *António Enes* (Imagem 3). Os oficiais desses navios e o Oficial de Dia à BNL estavam avisados da natureza deste exercício, mas as respetivas guarnições não, de modo a que as suas reações fossem as mais naturais possível. Contou-se ainda com o apoio do Centro de Investigação Naval (CINAV) e do Centro Integrado de Treino e Avaliação Naval (CITAN). Para efetuar o registo dos acontecimentos foi organizada uma equipa de observadores, composta por cinco elementos.

Figura 11 UAS COTS Parrot Bebop 2 FPV

Imagem 12 - UAS COTS Parrot Disco FPV

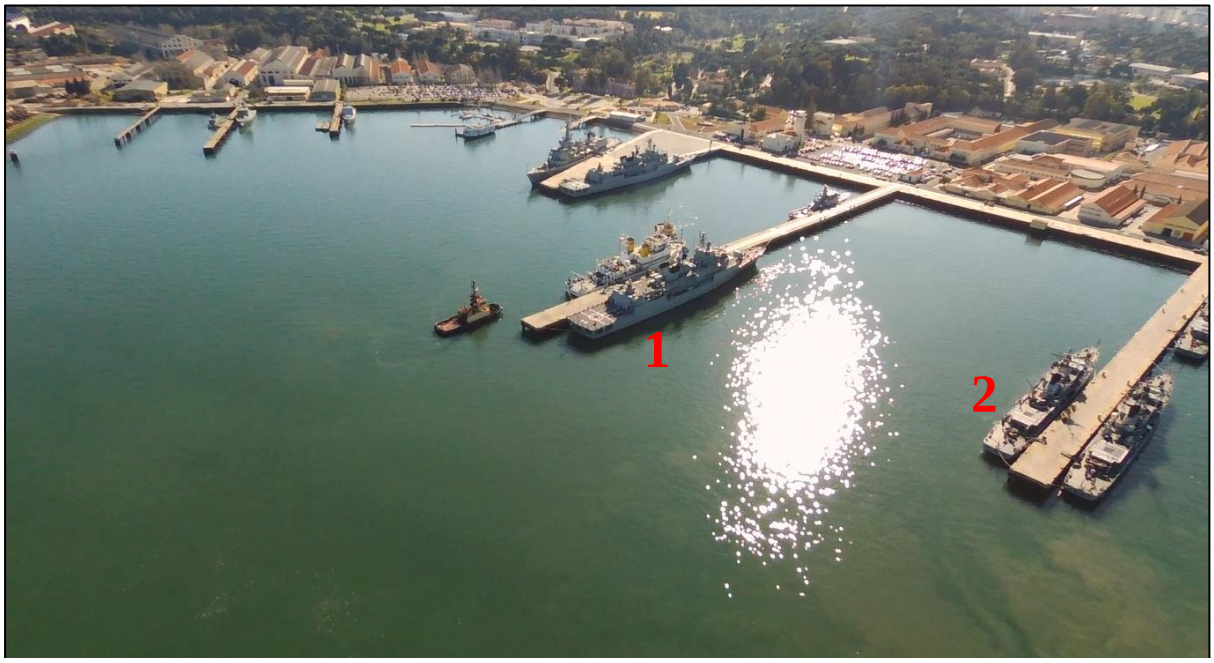


Figura 10 Imagem da Base Naval de Lisboa, obtida pelo Parrot Disco FPV. Note-se na posição 1 o NRP Vasco da Gama e na posição 2 o NRP António Enes. Fonte: UAS COTS operado pelos autores.

3. Descrição dos testes

Os testes estavam inicialmente previstos para a manhã de dia 12 de fevereiro. No entanto, os fortes ventos que se faziam sentir na zona e que impediam o voo dos UAS, obrigaram a adiar o exercício para a parte da tarde, das 1430 às 1540.

Durante a realização dos testes, o céu encontrava-se limpo, sem precipitação, o vento estava de norte com velocidade de 5 nós, a visibilidade era muito boa e temperatura era de 14ºC.

Pelas 1442 dá-se início ao exercício, com o lançamento do UAV 1 do cais 8 (ver Imagem 4), que inicia o perfil de voo para atingir a altitude dos 120 metros. No minuto a seguir, o UAV 1 é avistado pela Equipa de Observadores do NRP *Vasco da Gama*, estando o UAV 1 nesse momento a 222 m da ponta do cais nº3 da BNL. Há mesma hora,

Imagem 13 - Imagem da Base Naval de Lisboa, obtida pelo Parrot Disco FPV. Note-se na posição 1 o NRP Vasco da Gama e na posição 2 o NRP António Enes. Fonte: UAS COTS operado pelos autores.

o Oficial de Dia do NRP *Bérrio* contacta o Oficial de Dia à BNL, informando-o que dois Aspirantes a Oficial se encontram a operar um UAV no cais 8.

Às 1444, o UAV 1 inicia a aproximação ao NRP *Vasco da Gama*, com o rumo de 188 e altitude de 120 metros, sendo o mesmo detetado pelo Oficial de Dia desse navio, pelas 1445. Este tenta contactar, por rádio e telefone, o Comando Naval, mas sem sucesso. Quando o UAV1 inicia nova aproximação, a 100 m de altitude, o Oficial de Dia do NRP *Vasco da Gama* consegue finalmente contactar o Oficial de Dia à BNL via telemóvel e informa-o do avistamento do UAV1. Nesse preciso momento, o grupo de serviço desse navio perde o contacto visual com o UAV 1.

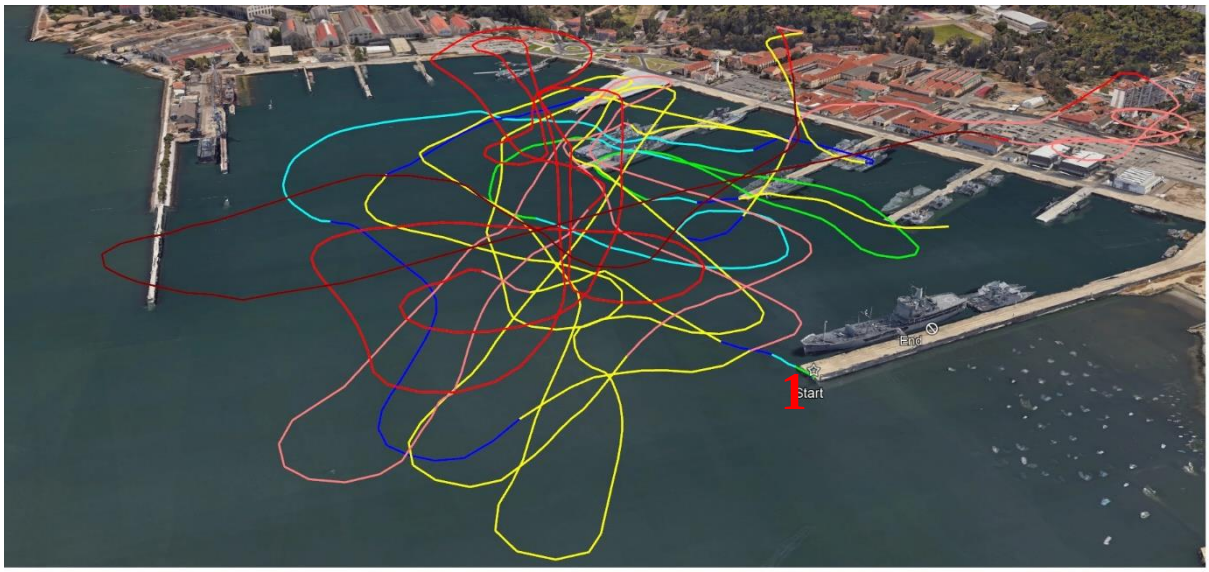


Figura 14 - Percurso realizado pelo Parrot Disco durante o exercício. Note-se que o mesmo foi lançado na posição1.

Pelas 1449 o UAV 1 inicia uma aproximação a 80 m de altitude e às 1451 realiza outra à mesma altitude. Só na segunda aproximação é que o Oficial de Dia do NRP *António Enes* avista o UAV 1 e informa o Oficial de Dia à BNL. Não são tomadas nenhumas outras medidas.

Seguidamente às 1453 o UAV1 inicia nova aproximação a 60 m de altitude, sendo somente detetado às 1454 pela guarnição do NRP *Vasco da Gama*, à distância de 312 m ao cais nº3.

Pelas 1455 é iniciada uma aproximação a 40 m de altitude, pelo UAV 1, sendo que a guarnição do NRP *António Enes* que se encontra na tolda avista o UAV 1, mas não o reporta. Logo de seguida o operador do UAV1 perde a ligação com o mesmo, recuperando-a dois minutos depois, devido á capacidade do UAV de retornar automaticamente ao ponto de lançamento.

Às 1500 efetua-se nova aproximação pelo UAV 1, esta a 20 m de altitude, e mais uma vez a guarnição do NRP *António Enes* não reporta a presença e movimentos do mesmo. O UAV 1 dirige-se então para o ponto de aterragem, onde pousa às 1507.

Pelas 1517 o UAV 2 levanta voo para a realização de aproximações a baixa altitude. É detetado pela guarnição do NRP *António Enes*, mas não é dado o alarme pela mesma. Devido à necessidade de verificar os sensores de altitude do UAV 2, que não se encontravam a transmitir dados, procede-se à sua aterragem.

Às 1522, o UAV 2 levanta voo novamente para efetuar duas novas aproximações com o objetivo de testar o equipamento de *jamming* presente no NRP *Vasco da Gama*, sendo que o mesmo se verificou eficaz, deixando o UAV 2 sem sinal e a realizar voo estacionário junto ao navio. O exercício teve o seu término pelas 1535.

Os dados recolhidos durante este exercício estão nos seguintes ficheiros de dados:

Embora o ficheiro de voo tenha sido retirado a partir do perfil de utilizador convertido pela *cloud* da Parrot, os mesmos dados podem ser retirados através do serviço FTP pelo ip 192.168.1.2121. ligando acedendo pela rede Wifi do UAV COTS, utilizando um PC.

UAV1.json - Ficheiro gerado pelo sistema de *cloud*, da Parrot que recebe os dados de voo do "Parrot Disco", com dados recolhidos pelos sensores do UAV. Este ficheiro, em formato próprio da Parrot, tem de segundo a segundo (ou seja, a 1Hz), a percentagem de bateria, posição da longitude (em graus) do controlador, posição da latitude (em graus) do controlador, estado da propulsão, alertas, estado do sinal wifi (em dB), estado do sinal de satélite, longitude (em graus), latitude (em graus), erro do posicionamento GPS, numero de satélites visíveis, velocidade em relação ao solo (em m/s), velocidade do vento (em m/s) retirado pelo Pitot tube, velocidade em x, velocidade em y, velocidade em z, estas velocidades (em m/s) adquiridas a partir do acelerómetro, Roll (em graus), Pitch (em graus), Yaw (em graus), estes três dados são adquiridos pelo giroscópio, altitude (em m) adquirida pelo altímetro.

UAV1.csv – Ficheiro em formato Excel com todos os dados extraídos do ficheiro anterior. Neste ficheiro cada linha corresponda a um instante segundo, e as colunas têm cabeçalhos autoexplicativos, com a informação descrita no parágrafo anterior. Este ficheiro foi obtido usado o programa: FlightData Manager – for Parrot Anafi, Parrot Bebop and Parrot Disco – Versão 4.1.8, que converte o ficheiro de voo JSON em CSV e KML.

UAV1.kml – Ficheiro com a trajetória para visualizar no Google Earth ou outro sistema GIS. Este ficheiro foi obtido usando o programa FlightData Manager – for Parrot Anafi, Parrot Bebop and Parrot Disco – Versão 4.1.8, que converte o ficheiro de voo JSON em CSV e KML, criando assim um ficheiro com os caminhos realizados pelo Parrot Disco.

4. Conclusões

As conclusões obtidas, de acordo com os objetivos estipulados no início, foram as seguintes:

a) Quando um elemento da guarnição avista um UAS nas imediações do seu navio, avisa o Oficial de Dia, que por sua vez contacta com o Oficial de Dia à BNL. No entanto este procedimento só foi efetuado na primeira vez que se detetou o UAS.
b) Os UAS não são considerados uma ameaça por parte das guarnições dos navios. Mesmo depois de ter avistado os UAS COTS, a guarnição manteve-se no exterior dos navios, tendo-se até juntado mais pessoal para observar as aeronaves. Tal despreocupação deve-se a dois motivos principais: o desconhecimento das capacidades bélicas dos UAS COTS e a sua associação a simples brinquedos.
c) Para além de informarem o Oficial de Dia, os militares da guarnição não tomaram mais alguma medida e não se preocuparam em manter um constante contacto visual com o UAS COTS, tendo-o perdido várias vezes.
d) Para além da comunicação do avistamento do UAS COTS para o Oficial de Dia à BNL, não existem outros procedimentos a executar por parte do navio.
e) Os sensores eletro-óticos de ambos os UAS COTS mostraram ser capazes de, independentemente da altitude a que operaram, recolherem imagens precisas e discriminadas do ambiente portuário. Quanto à capacidade de manobra, o UAS COTS de asa rotativa mostrou-se mais prático, devido à sua capacidade de conseguir pairar sobre um ponto. O UAS COTS de asa fixa é mais rápido (conseguiu atingir 68 km/h) e é melhor para fazer o varrimento de grandes áreas, através de fiadas. O de asa rotativa tem maior aceleração e é melhor para realizar observações focadas num determinado ponto.
f) Durante a realização dos testes, houve perda do sinal de controlo do UAS COTS de asa fixa devido à superestrutura do NRP Bérrio se encontrar entre o operador e a aeronave. Assim, recomenda-se que o operador esteja afastado de infraestruturas altas durante a operação destes modelos.
g) O UAS COTS de asa fixa percorreu 16 km durante os 20 minutos de voo. Quando aterrou, a percentagem de bateria que sobrou era de 48%.
h) O equipamento de *jamming* foi eficaz a neutralizar a potencial ameaça do UAS. O UAV 2 efetuou duas aproximações em direção ao *jammer*, tendo este conseguido afetar o sinal de controlo, fazendo com que o UAV 2 se afastasse do navio e ficasse em voo estacionário nas imediações, a potência utilizada pelo *jammer* foi de 1 W, sendo que a frequência afetada foi a Wifi (2.4Ghz), o método utilizado foi ruido Gaussiano.

As lições retiradas deste teste permitiram completar as dissertações de mestrado em questão.

Ficou comprovado que os UAS COTS podem desempenhar um papel importante em ações de vigilância e reconhecimento. A sua capacidade de transmitir imagem em tempo real permite ajudar a coordenar ações ofensivas contra instalações portuárias, enquanto que a sua reduzida silhueta os torna difíceis de detetar e seguir, o que lhes confere vantagem tática na aproximação ao alvo. Através dos dados retirados pelos sensores do UAV1, pode-se constatar a relação que existe entre as manobras executadas durante o exercício e a autonomia do UAV1 (ver gráfico 1).

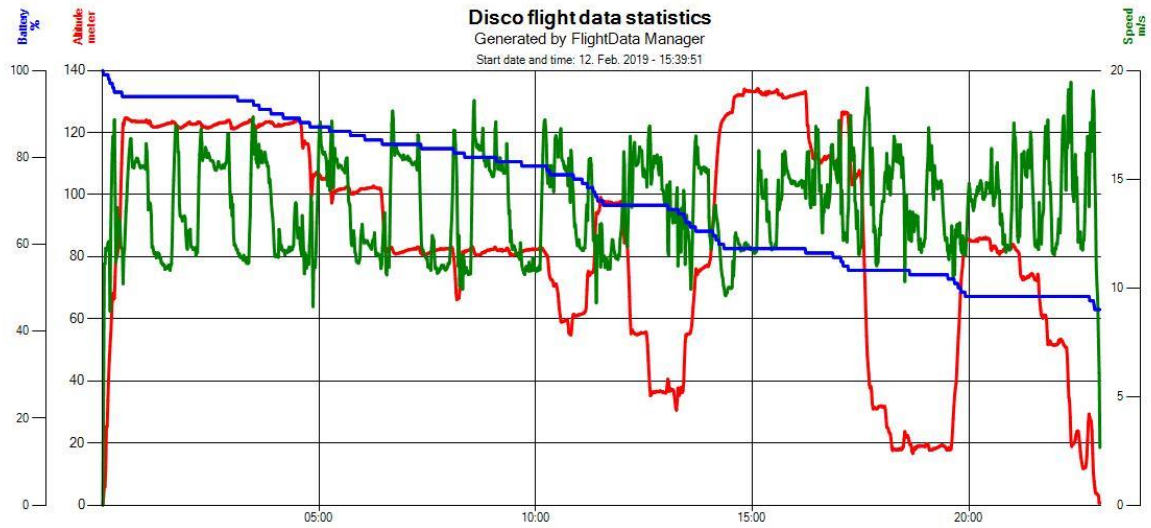


Gráfico 1 – Relação entre bateria (gráfico azul), altitude (gráfico vermelho) e velocidade (gráfico verde) do Parrot Bebop FPV

Na análise do gráfico anterior é possível concluir que, quando se dão variações ascendentes de altitude é quando ocorre o maior decréscimo de percentagem de bateria. Concluindo assim que durante a operação de UAS COTS, a forma como são realizados os perfis de voo, devem ser o menos variáveis em altitude (principalmente ascendente), para assim poder ser aproveitado au máximo a autonomia deste modelo de UAS COTS.

Concluiu-se que a utilização de UAS COTS em operações militares ou terroristas, por ser ainda um tema recente, não é percecionada como uma ameaça pelas guarnições dos navios. Os elementos a bordo não se deslocaram para uma posição protegida e não se preocuparam em relatar constantemente a posição da aeronave. Tal se deve ao facto de ainda olharem para os UAS COTS como um brinquedo e não compreenderem/não terem conhecimento dos potenciais perigos que lhes estão associados. Os oficiais de dia agiram corretamente, e seguiram as (poucas) instruções que tinham. É de notar que, para além do NRP *Bérrio* (cujo Oficial de Dia avistou logo no início dos testes os dois operadores dos

UAV no cais 8) e dos dois navios que faziam parte do exercício, nenhum outro navio comunicou para o Oficial de Dia à BNL qualquer avistamento de UAV. Tal pode-se dever a duas situações: ou os UAV não foram avistados por outros navios, ou foram avistados, mas não se informou quem de direito.

Provou-se também que um sistema de *jamming* é bastante eficaz contra este tipo de ameaça, podendo vir a ocupar um papel central na defesa anti UAS COTS.