INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE PROMOÇÃO A OFICIAL SUPERIOR - MARINHA

2016/2017

TII

PCOP
CONCEITO DE UMA COP PARA APOIO AO COMANDO E CONTROLO DE FORÇAS NACIONAIS CONJUNTAS

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IUM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS OU DA GUARDA NACIONAL REPUBLICANA.

Luís Quaresma dos Santos

1TEN TSN

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

PCOP
CONCEITO DE UMA COP PARA APOIO AO COMANDO E CONTROLO DE FORÇAS NACIONAIS CONJUNTAS

1TEN TSN Luís Quaresma Dos Santos

Trabalho de Investigação Individual do CPOS-M 2016/2017

Pedrouços 2017

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

PCOP
CONCEITO DE UMA COP PARA APOIO AO COMANDO E CONTROLO DE FORÇAS NACIONAIS CONJUNTAS

1TEN TSN Luís Quaresma Dos Santos

Trabalho de Investigação Individual do CPOS-M 2016/2017

Orientador: CFR SEP António José Sempiterno Ribeiro

Pedrouços 2017

Declaração de compromisso antiplágio

Eu, **Luís Quaresma dos Santos**, declaro por minha honra, que o documento intitulado "**PCOP - Conceito de uma COP para apoio ao comando e controlo de forças nacionais conjuntas**", corresponde ao resultado da investigação por mim desenvolvida, enquanto auditor do **CPOS - Marinha 2016-17,** no Instituto Universitário Militar e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços**, 18** de **Junho** de **2017**

Luís Quaresma dos Santos

Agradecimentos

Agradeço ao CRF Sempiterno Ribeiro, meu orientador neste trabalho, por todo o apoio facultado e entusiasmo colocado na investigação. Com ele, aprendi muito da arte da gestão moderna de projetos e em particular da sua aplicação prática em projetos concretos das nossas Forças Armadas.

Peço desculpa à Carla, ao Afonso, ao Manuel e ao António pelo tempo que não passei com eles neste último ano.

Índice

Índice de Anexos

Índice de Apêndices

Índice de Figuras

Índice de Tabelas

Resumo

O presente estudo constrói o conceito de uma *Portuguese Common Operational Picture* (PCOP) para dar resposta às necessidades de gestão da informação operacional, do Comando Conjunto para as Operações Militares (CCOM) no apoio ao Comando e Controlo (C2) de forças nacionais conjuntas. O conceito é construído seguindo os processos que constituem a fase de iniciação da gestão moderna de projetos e alinhado com normas internacionais e a doutrina militar, nacional e NATO. Desenvolve-se a definição do âmbito inicial do produto, a identificação dos *stakeholders* do projeto, a elaboração de um conceito de operação e o levantamento dos requisitos críticos da PCOP. A solução encontrada, procura explorar as capacidades já existentes nos ramos, de forma a reduzir os custos do projeto e a envolver as FFAA neste esforço, que se deseja conjunto.

Este trabalho pretende dar visibilidade à necessidade de se construir uma PCOP, ajudando a definir a visão do projeto (*o que é necessário fazer?*). As caraterísticas principais da PCOP são definidas e os requisitos críticos principais identificados, a ter em conta no seu desenho e construção. Caberá ao patrocinador, na fase que se segue, decidir se este projeto deve ser desenvolvido, repensado ou abandonado.

Palavras-chave: *common operational picture*, comando e controlo, gestão de projeto, *ConOps*, CCOM.

Abstract

The present study builds the concept of a Portuguese Common Operational Picture (PCOP) to address the operational information management, needed by the Portuguese Joint Command for Military Operations (CCOM) to support the Command and Control (C2) of national forces acting together. The concept is built following the processes that comprise the initiation phase of modern project management and in line with international standards and military doctrine. It develops the Initial Product Scope; Identify Stakeholders, Concepts of Operations and High-level Critical Requirements for the PCOP project. The solution found seeks to exploit the already existing capabilities in the national military structure, in order to reduce project costs and to involve the all the Portuguese Armed Forces in this joint effort.

This work aims to give visibility to the need for build a PCOP and to help define the vision of the project (what needs to be done?). PCOP main features are defined and major critical requirements are identified, to take into account during the design of the product and its construction. It will be up to the sponsor, in the next step, to decide whether this project should be developed, rethought or abandoned.

Keywords: *common operational picture, command & control, project management, ConOps,* CCOM.

Lista de abreviaturas, siglas e acrónimos

ACCS *Air Command and Control System* (NATO)

AirC2IS *Air Command and Control Information System* (NATO)

AIR *Area of Intelligence Responsibility*

AOI *Area of Interest*

AOO *Area Of Operations*

AOR *Area Of Responsibility*

BMS *Battlefield Management System* (Exército)

CC Carros de Combate

C2 Comando e Controlo

C3 Comando, Controlo e Comunicações

CA Comando Aéreo

CCOM Comando Conjunto para as Operações Militares

CEM Conceito Estratégico Militar

CEMA Chefe do Estado-Maior da Armada

CEMCCOM Chefe do Estado-Maior do Comando Conjunto para as Operações Militares

CEME Chefe do Estado-Maior do Exército

CEMGFA Chefe do Estado-Maior General das Forças Armadas

CEMFA Chefe do Estado-Maior da Força Aérea

CIMIC Cooperação Civil-Militar

CFT Comando das Forças Terrestres

CIGEOE Centro de Informação Geográfica do Exército

CIMFA Centro de Informação Meteorológica da Força Aérea

CIS *Communications and Information Systems*

CISMIL Centro de Informações e Segurança Militares

CJTF *Combined Joint Task Force*

CMF Conjunto Modular de Forças

COA Comando Operacional dos Açores

COC Centro de Operações Conjunto

COM Comando Operacional da Madeira

COMNAV Comando Naval

COP *Common Operational Picture*

COSF Componente Operacional do Sistema de Forças nacional

CPOE Célula de Planeamento de Operações Especiais

CS Conhecimento Situacional

CTAC Centro de Treino, Avaliação e Certificação

CTF *Combined Task Force*

DCSI-E Direção de Comunicações e Sistemas de Informação (Exército)

DCSI-F Direção de Comunicações e Sistemas de Informação (Força Aérea)

DGRDN Direção Geral de Recursos de Defesa Nacional (MDN)

DIRCSI Direção de Comunicações e Sistemas de Informação

DITIC Direção de Tecnologias de Informação e Comunicações (Marinha)

EMCCOM Estado-Maior do Comando Conjunto para as Operações Militares

FAP Força Aérea Portuguesa

FPAS Forças Permanentes em Ação de Soberania

FFAA Forças Armadas

FNC Forças Nacionais Conjuntas

FND Forças Nacionais Destacadas

FRI Força de Reação Imediata

ICC *Integrated Command and Control Software for Air Operations* (NATO)

IH Instituto Hidrográfico (Marinha)

I&D Investigação e Desenvolvimento

J1 Célula do Pessoal (Estado-Maior)

J2 Célula das Informações (Estado-Maior)

J3 Célula das Operações (Estado-Maior)

J4 Célula da Logística (Estado-Maior)

J5 Célula dos Planos (Estado-Maior)

J6 Célula da Comunicações (Estado-Maior)

J7 Célula das Finanças (Estado-Maior)

J8 Célula do Treino (Estado-Maior)

J9 Célula da Cooperação Civil-Militar (Estado-Maior)

JIP *Joint Intelligence Picture*

JOA *Joint Operations Area*

JOP *Joint Operations Picture*

JTLP *Recognized Theatre Logistic Picture*

KD *Knowledge Development*

LC2IS *Land Command and Control Information Service* (NATO)

MCCIS *Maritime Command and Control Information System* (NATO)

METOC *Meteorology and oceanography*

METOCMIL Meteorologia e Oceanografia Militar

MRO *Military Response Option*

MDN Ministério da Defesa Nacional

NATO *North Atlantic Treaty Organization*

NBQR Defesa Nuclear Biológica Química e Radiológica

OA *Objective Area*

OE Objetivo Específico

OG Objetivo Geral

PCOP *Portuguese Common Operational Picture*

RAP *Recognized Air Picture*

REP *Recognized Environmental Picture*

RJP *Recognized Joint Picture*

RTLP *Recognized Theatre Logistics Picture*

RSFP *Recognized Special Forces Picture*

ROE *Rules of Engagement*

SIC Sistemas de Informação e de Comunicação

SIG Sistemas de Informação Geográfica

SOF *Special Operations Forces*

TO Teatro de Operações

UNAVE Unidade Nacional de Verificações

Introdução

Na era da informação, o conhecimento surge como fator determinante para o sucesso das operações militares. Forças Armadas (FFAA) mais rápidas, letais e precisas necessitam de um Comando e Controlo (C2) pronto e eficaz, apenas possível quando apoiado por informação relevante, clara e segura (Joint Vision 2020, 2000). A crescente necessidade de acesso a informação em tempo real, obriga a um desenvolvimento tecnológico que acompanhe a transformação das plataformas e dos sistemas de armas, assim como a velocidade do seu emprego, a flexibilidade da sua atuação e as diversas configurações do seu comando conjunto e combinado (Figura 1).

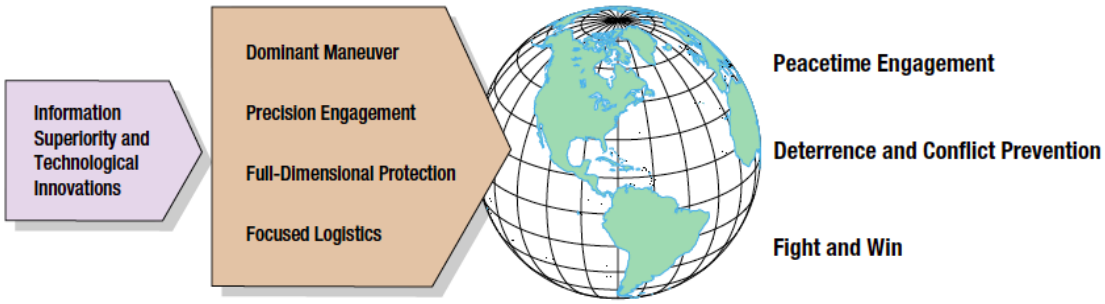

Figura 1 – A superioridade de informação no espetro da guerra.

Fonte: (Joint2020, 2000)

Enquadramento e justificação do tema

À semelhança de outros países que integram a Organização do Tratado do Atlântico Norte (NATO[1]), Portugal procura transformar as suas FFAA numa organização moderna e sustentável. Esta estratégia foi recentemente publicada (Defesa 2020, 2015) e define como nível de ambição, privilegiar um sistema de forças organizado em capacidades conjuntas, modulares e flexíveis, assente em requisitos de prontidão e de continuidade. Consequentemente, as FFAA foram reorganizadas a partir da criação de um Comando Conjunto para as Operações Militares (CCOM), munido da missão de apoiar o CEMGFA[2] no comando das forças e meios da Componente Operacional do Sistema de Forças (COSF) (Decreto-Lei 184, 2014). O CCOM constitui um comando permanente de nível operacional, sustentado pela partilha de meios e recursos disponibilizados pelos Ramos (Marinha, Exército e Força Aérea). A *Defesa2020* preconiza também uma transformação das capacidades C2 das FFAA, destacando-se a proposta de criação de um serviço

[1] adota-se neste trabalho o acrónimo em inglês
[2] Chefe do Estado-Maior General das Forças Armadas

coordenador comum das Comunicações e dos Sistemas de Informação (CIS), apto a centralizar, num único pólo, uma plataforma transversal de apoio à decisão operacional.

O presente trabalho de investigação pretende contribuir para a operacionalização deste objetivo estratégico, desenvolvendo o conceito de uma *Portuguese Common Operational Picture* (PCOP), no apoio às funções C2 do CCOM. Este tema insere-se no domínio de investigação das Ciências Militares, na área das Técnicas e Tecnologias Militares e na subárea Comando, Controlo, Comunicações, Computadores e Informação.

Objeto de estudo e delimitação

Selecionou-se como objeto de estudo a PCOP, enquanto ferramenta de integração, georreferenciação e Conhecimento Situacional (CS) dos Teatros de Operações (TO) conjuntos. Limitou-se este objeto à fase de iniciação de um projeto de desenvolvimento de novos sistemas, que corresponde à fase de conceptualização do produto (Apêndice A). Esta fase, integra um conjunto de processos que vão ajudar o patrocinador a decidir pela continuidade do projeto[3]. Constituem estes processos: a definição do âmbito inicial do produto a desenvolver; a identificação das partes interessadas no projeto[4]; a elaboração de um conceito de operação e o levantamento dos requisitos críticos do produto (PMI, 2013).

Objetivos da investigação

Esta investigação teve por Objetivo Geral (OG), explorar o conceito da PCOP, seguindo os processos da fase de iniciação da gestão moderna de projetos (PMI, 2013) e pelas normas internacionais (ISO/IEC/IEEE, 2015; INCOSE, 2012). A investigação norteou-se pela pergunta de partida: *Como deve ser definida a PCOP para responder da melhor forma às necessidades C2 do CCOM?*

Questões da investigação

Para alcançar o OG, o trabalho foi decomposto nos quatro processos que compõem a fase de conceptualização, constituindo os seus resultados os Objetivos Específicos (OE) do estudo. Cada OE pode ser apresentado na forma de Questões Derivadas (QD), adotando o método de observação crítica *Golden Circle* (Sisney, 2012), baseado nas questões: *Who?*, *Why? What? e How?*:

[3] se positivo, o projeto segue para as fases de planeamento, execução e, por fim, operacionalização ou comercialização do produto.

[4] *stakeholders*

QD1: *Porque necessita o cliente da ferramenta?*

OE1: Definição do âmbito da PCOP determinado (*Why?*);

QD2: *Quem afeta ou é afetado pela ferramenta?*

OE2: *Stakeholders* da PCOP identificados (*Who?*);

QD3: *O que vai fazer a PCOP?*

OE3: Conceito de operação da PCOP definido (*What?*);

QD4: *Como deve operar a ferramenta?*

OE 4: Requisitos críticos da PCOP levantados (*How?*).

Metodologia de investigação

A definição do Objeto de Estudo e a delimitação do OG e dos OE orientaram a metodologia e os instrumentos de análise utilizados no trabalho. A investigação seguiu um raciocínio do tipo "pensamento crítico", adoptando a "reflexão" como método de análise objetiva e criteriosa (Paul & Elder, 2006). Seguiu uma estratégia qualitativa, baseada na recolha de informação, dados e elementos que se julgaram suficientes para construir o conceito da PCOP, construído a partir das respostas à pergunta de partida e questões derivadas. O desenho de pesquisa escolhido assentou num "caso de estudo", focado na aplicação do seu Objeto à realidade e necessidade atual das FFAA portuguesas (horizonte temporal). O resultado do estudo não pretende generalizar a solução encontrada para outras forças, nacionais ou estrangeiras, mas sim encontrar uma solução concreta e exequível para responder às necessidade do CCOM.

O estudo seguiu o percurso metodológico estabelecido na NEP/ACA-010 (IUM, 2015), dividido em três fases: exploratória, analítica e conclusiva. Utilizou como técnica de recolha de dados, a observação estruturada, a entrevista não estruturada (fase exploratória) e estruturada (fase analítica) e a análise documental. A interpretação dos resultados foi realizada recorrendo à reflexão crítica do autor, apoiada pelo orientador e validada por especialistas na matéria[5].

Na fase exploratória, recolheu-se informação dispersa sobre CIS aplicados ao C2 de forças aliadas. Foram realizadas entrevistas não estruturadas a elementos da componente operacional dos três ramos (COMNAV[6], CA[7] e CFT[8]) e a elementos da componente técnica da Marinha (DITIC[9]) e do Exército (DCSI-E[10]).

[5] representantes dos principais *stakeholders* da PCOP
[6] Comando Naval
[7] Comando Aéreo

Na fase analítica efetuou-se uma análise documental orientada para a construção do conceito da PCOP, nomeadamente doutrina nacional, NATO e de outros países aliados. Foram realizadas observações e entrevistas estruturadas à estrutura do CCOM, CISMIL[11] e DIRCSI[12].

Na fase conclusiva, elaboraram-se os produtos que desenham o conceito da PCOP (OG), recorrendo à análise crítica dos resultados alcançados em cada OE e após validação por parte do CCOM[13].

Estrutura do trabalho

O trabalho está organizado em quatro capítulos que correspondem aos produtos resultantes dos processos, que compõem a fase conceptual do ciclo de desenvolvimento da PCOP, e que conduzem à elaboração do seu conceito. No capítulo 1 (Definição do âmbito da PCOP) é respondida à QD1: *Porque necessita o cliente da ferramenta?*; no capítulo 2 (Identificação de stakeholders da PCOP) é respondida à QD2: *Quem afeta ou é afetado pela ferramenta?*; no capítulo 3 (Conceito de operação da PCOP) é respondida à QD3: *O que vai fazer a ferramenta?*; no capítulo 4 (Requisitos críticos da PCOP) é respondida À QD4: *Como deve operar a ferramenta?*.

[8] Comando das Forças Terrestres
[9] Direção de Tecnologias de Informação e Comunicação
[10] Direção de Comunicações e Sistemas de Informação
[11] Centro de Informações e Segurança Militar (EMGFA)
[12] Direção de Comunicações e Sistemas de Informação (EMGFA)
[13] representado pelo CEMCCOM

1. Definição do âmbito da PCOP

A definição do âmbito inicial de um novo produto, ou sistema, constitui o processo pelo qual se esclarecem, determinam e acordam as suas características principais. Seguindo a boa prática da gestão avançada de projetos (PMI, 2013), a definição do âmbito da PCOP foi realizada, em conjunto com o CCOM (cliente), através de entrevistas estruturadas, realizadas ao Chefe da Área de Operações do EMCCOM e ao Comandante da Força de Reação Imediata (FRI). A análise das entrevistas permitiu selecionar os pontos chave do problema a resolver. A apreciação da legislação que regula o CCOM (Decreto-Lei 184, 2014), da doutrina militar conjunta nacional (PDMC-01, 2012) e NATO (NATO AJP-6, 2011), definiram o âmbito da PCOP, a partir das funções que se lhe consideram determinantes.

1.1 **Recolha, integração e análise de informação operacional**

O CCOM é regulado por legislação própria. Tem por missão "assegurar o exercício, por parte do CEMGFA, do comando operacional das forças e meios da COSF, em todo o tipo de situações e para as missões das FFAA". Este comando deve manter articulação funcional permanente com os ramos, em todas as fases operacionais, incluindo preparação, apontamento, planeamento, execução, controlo, sustentação e retração das Forças Nacionais Conjuntas (FNC).

O CCOM é chefiado pelo Chefe do Estado-Maior do Comando Conjunto para as Operações Militares (CEMCCOM) e apoiado por um Estado-Maior (EMCCOM). Integra uma Célula de Planeamento de Operações Especiais (CPOE), o Centro de Treino, Avaliação e Certificação (CTAC) e a Unidade Nacional de Verificações (UNAVE).

Para articular, coordenar e dirigir o emprego da COSF, o CEMGFA necessita de desenvolver um conjunto de capacidades (*CEM*, 2014), onde se incluem C2 e CS. O desenvolvimento destas duas capacidades está ainda longe do nível de ambição nacional (Defesa 2020, 2015), identificando-se como imperativa a necessidade de construir um sistema de informação geoespacial, capaz de recolher, integrar e analisar a vasta informação que é produzida pelos diferentes elementos da COSF e do CCOM, no sentido de proporcionar uma perceção comum do ambiente operacional e incrementar a capacidade C2 do CEMGFA.

1.2 **Partilha vertical de informação**

O EMCCOM tem por missão planear e coordenar o emprego das forças e meios da COSF em operações militares, apoiando o CEMGFA na sua ação de comando operacional

(Decreto-Lei 184, 2014). Compete ao EMCCOM a função de controlo de todas as forças e meios da COSF, nomeadamente quando, na dependência do CEMGFA, se encontram fora do território nacional. Este função deve traduzir-se numa capacidade efetiva em acompanhar o emprego, sustentação, projeção e retração da COSF.

1.2.1 Nível Operacional

Em situação de paz, o CEMGFA é o comandante operacional das FFAA e o responsável pelo seu emprego no cumprimento das missões, em território nacional e no estrangeiro, incluindo a cooperação com as forças e serviços de segurança nacionais, bem como em missões de proteção civil (Decreto-Lei 184, 2014). O CEMGFA tem como subordinados diretos os comandantes das forças e meios, que se constituam na sua dependência, bem como os "comandos de componente dos ramos", de acordo com as modalidades C2 aplicáveis no quadro legislativo.

São também comandos de nível operacional e natureza conjunta, o Comando Operacional dos Açores (COA) e da Madeira (COM). Têm por missão efetuar o planeamento, o treino operacional conjunto e o emprego operacional das forças e meios que lhe sejam atribuídos pelo CEMGFA. Compete-lhes planear e executar as medidas superiormente aprovadas, relativas à defesa militar dos respetivos arquipélagos.

1.2.2 Nível Estratégico

Para além de comandante operacional, o CEMGFA é também a autoridade militar responsável pelo nível estratégico (PDMC-01, 2012). É responsável pelo planeamento e implementação da estratégia militar e tem na sua direta dependência hierárquica os Chefes de Estado-Maior dos ramos, para o apoiar nas funções de aprontamento, emprego e sustentação das forças e meios da COSF. Em situação de guerra, o CEMGFA exerce, sob a autoridade do Presidente da República e do Governo, o comando completo das FFAA (Decreto-Lei 184, 2014). É da sua responsabilidade a elaboração dos planos de defesa militares e dos planos de contingência, a definição dos TO e das Áreas de Operações Conjuntas (JOA), assim como a nomeação, ou exoneração, dos comandantes nos TO, bem como a definição das suas competências, forças e meios a outorgar-lhes por carta de comando.

Estas responsabilidades de nível estratégico do CEMGFA revelam que é a este nível que se começa a organizar o campo de batalha, definindo as JOA, atribuindo meios e capacidades militares no espaço e no tempo. Se este planeamento for sustentado por informação geográfica, validada e analisada de forma integrada, o seu produto será de

extrema utilidade para a fase da condução das operações, ao nível operacional. Por outro lado, a informação gerada pelos níveis tático e operacional são importantes para apoiar o CEMGFA a assegurar-se que as operações, em curso, estão a contribuir para a consecução dos objetivos estratégicos militares. Esta informação é também importante para assessorar as decisões do nível político, em caso de eventuais alterações nos requisitos de forças, regras de empenhamento (ROE), áreas de projeção e termos de integração em operações combinadas (PDMC-01, 2012).

1.2.3 Nível Tático

A COSF agrupa as capacidades dos ramos numa estrutura de natureza conjunta, organizada em três grupos de forças (CEM, 2014):

a) A FRI, tem por missão a "evacuação de cidadãos nacionais, em áreas de crise, ou conflito, e de resposta nacional autónoma em situações de emergência complexas". Esta força está permanentemente ativa e pode atuar de forma autónoma, dispondo de um comandante, de nível tático, subordinado ao comando operacional do CEMGFA.

b) As Forças Permanentes em Ação de Soberania (FPAS) estão dirigidas para missões de patrulhamento, vigilância e fiscalização marítima e aérea, vigilância terrestre, defesa aérea, busca e salvamento, defesa Nuclear Biológica Química e Radiológica (NBQR), assim como outras de interesse público. As capacidades destas forças estão dispersas pelos ramos. Exercem o seu comando (tático) o respetivo Chefes do Estado-Maior do ramo a que pertencem, comandos estes que estão subordinados ao comando operacional por parte do CEMGFA.

c) O Conjunto Modular de Forças (CMF) constitui o agregado das forças e meios destacados em missões no exterior de Portugal (FND)[14]. É da responsabilidade do CCOM, no âmbito das competências do CEMGFA, acompanhar estas missões.

A COSF também integra Forças de Operações Especiais (SOF[15]), constituídas a partir de meios e unidades aprontadas pelos ramos. O seu planeamento, integração, sincronização e emprego é responsabilidade do CEMGFA, pelo que foi criada no CCOM

[14] Forças Nacionais Destacadas.
[15] *Special Operations Forces*

uma Célula permanente de Planeamento de Operações Especiais (CPOE). A CPOE constitui o núcleo inicial do comando de componente SOF.

Constata-se assim, a existência de várias forças, constituídas e previstas na doutrina (PDMC-01, 2012) e legislação (CEM, 2014), cujo comando operacional está a cargo do CEMGFA e o apoio é prestado pelo CCOM. Para um C2 eficaz, existe uma imperativa necessidade de partilhar informação entre os diferentes níveis de comando (Figura 2).

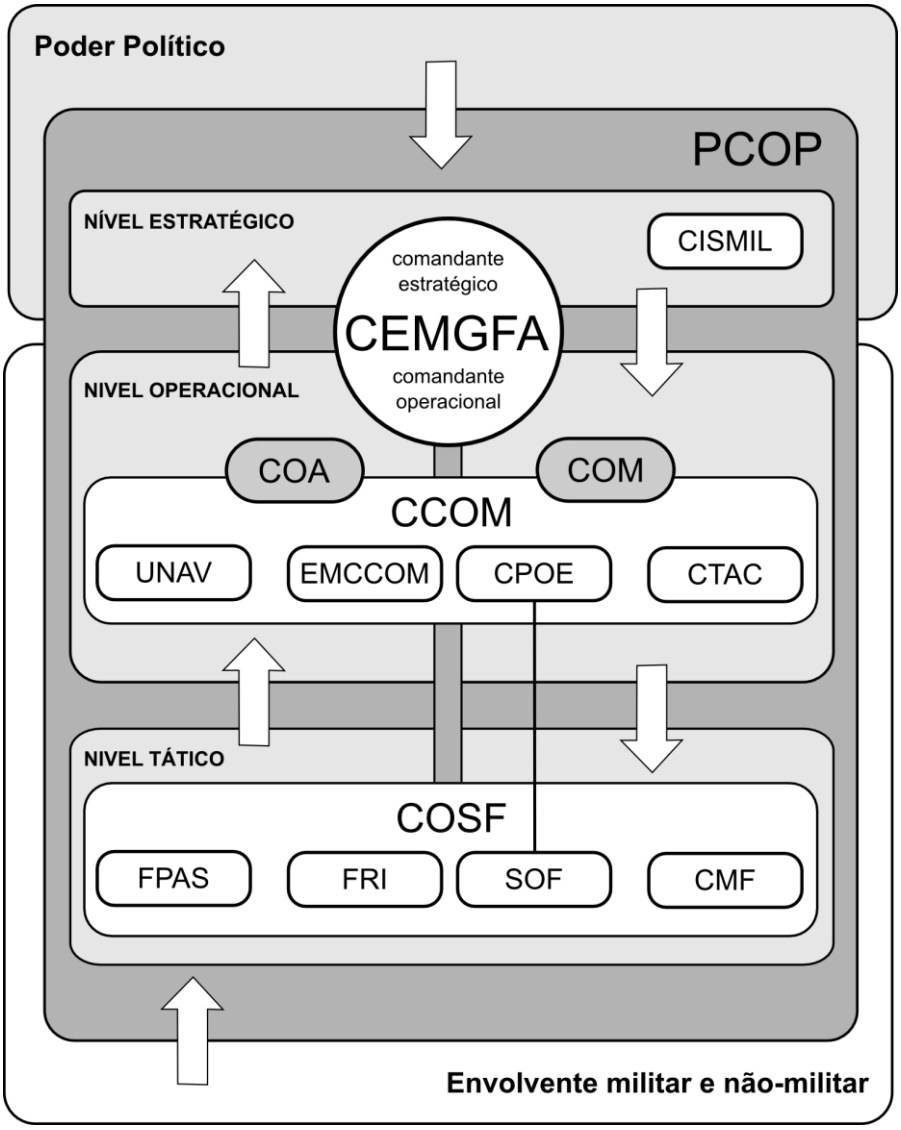

Figura 2 - Partilha vertical da informação ao longo da estrutura de comando do CEMGFA

Fonte: (autor, 2017)

1.3 **Partilha horizontal de informação**

O CCOM tem a missão de apoiar CEMGFA nas suas ações de comando. O seu Estado-Maior (EMCCOM) é formado por áreas, células e um centro de operações, que diariamente produzem todas a atividade necessária ao apoio desta competência operacional (Figure 2):

a) Na Área de Operações estão integrados o Centro de Operações Conjunto (COC) e as funções militares das Informações (J2) e das Operações Correntes (J3). O seu responsável acumula a chefia do COC.

b) Na Área de Planos estão integradas as funções militares dos Planos (J5), do Treino e Formação (J8), assim como da Cooperação Civil-Militar[16] (J9);

c) Na Área de Recursos estão integradas as funções do Pessoal (J1), da Logística (J4), das Comunicações (J6) e das Finanças (J7).

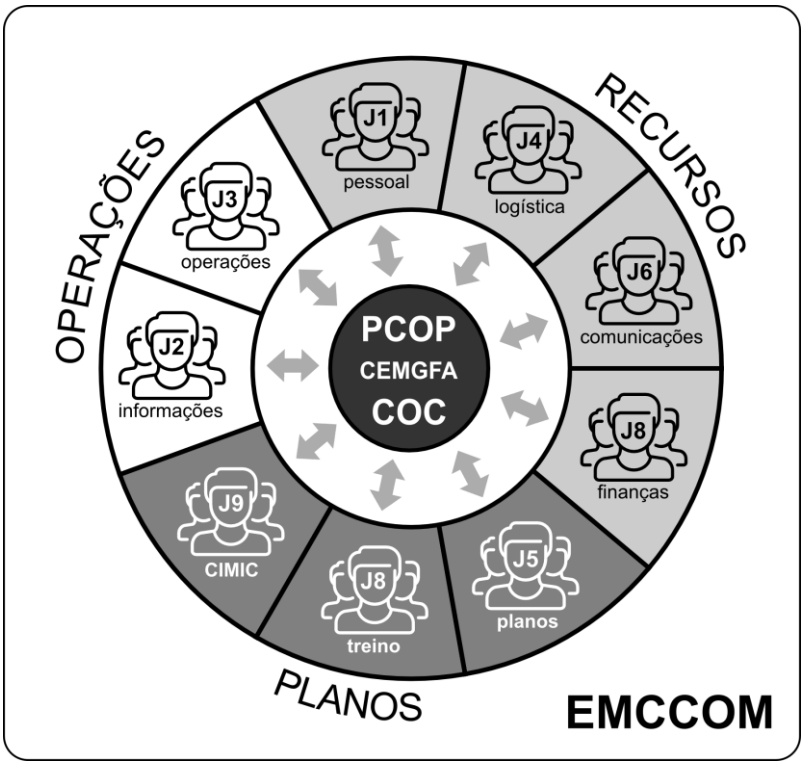

Figura 3 – Organização da partilha horizontal da informação.

Fonte: (autor, 2017)

[16] CIMIC

1.3.1 Centro de Operações Conjunto (COC)

O COC tem a responsabilidade de coordenar a execução das diretivas operacionais emanadas pelo CEMGFA, em operações militares externas e internas, assim como manter atualizada a informação relativa aos estados de prontidão, graus de disponibilidade e capacidades de sustentação para combate, tal como estabelecidos para as forças e meios da COSF. Compete ao COC, garantir a capacidade C2 das FFAA, assim como das Forças de Segurança, quando nos termos da lei estejam colocadas na dependência do CEMGFA. Cabe ainda ao COC garantir o CS nos TO e apresentá-la na forma de briefings de situação.

Verifica-se, que as competências do COC tornam-no no utilizador principal da PCOP, requerendo uma capacidade de localizar, quantificar e caracterizar as forças e os meios da COSF, assim como de integrar na COP informação proveniente de outras forças nacionais (Forças de Segurança e Proteção Civil) e externas (ex. Forças NATO e UE). Acrescem a estas necessidades as funções de visualização da informação, proveniente das forças e comandos de componentes, bem como da informação produzida pelas diferentes células que compõem o EMCCOM.

1.3.2 Pessoal (J1)

A J1 é responsável por todos os assuntos administrativos respeitantes à gestão dos recursos humanos (civis e militares) envolvidos nas operações militares a cargo do CEMGFA. No âmbito da PCOP, considera-se apoiar a J1 na integração e gestão da informação relativa ao pessoal em operação, associando à sua posição no TO, e no tempo, dados administrativos, tais como: quantitativos e movimentos de pessoal; necessidades de reforço ou substituição de pessoal nas unidades distribuídas pelo TO; estado de saúde, moral das tropas, entre outros;

1.3.3 Informações (J2)

À J2 compete garantir a avaliação do risco e da ameaça, nas áreas e TO onde se encontrem forças e elementos nacionais destacados (FND), assim como coordenar os esforços de pesquisa e análise das informações, empregando diferentes fontes e sistemas de informações[17]. No âmbito da PCOP, considera-se apoiar a J2 na integração e gestão das informações recolhidas nos TO, bem como de outras obtidas na área de interesse das operações, construindo assim um Panorama de Informações Conjunto (JIP)[18]. Constituem

[17] a J2 possui a responsabilidade de produzir, em articulação com o CISMIL, informações necessárias à preparação e execução de operações militares. Torna-se assim necessária partilha vertical de informação.

[18] *Joint Intelligence Picture*

funcionalidades a incluir na PCOP, as capacidades de registar e posicionar eventos, gerir o seu histórico, bem como executar análises de padrões e correlações.

1.3.4 Operações (J3)

À J3 compete a coordenação do emprego da COSF com vista a alcançar os objetivos definidos pelo CEMGFA. Deve, no decorrer das missões, organizar os meios e priorizar as ações previstas nos planos de operações, garantindo a máxima eficiência através da exploração de sinergias[19] no tempo e no espaço. No âmbito da PCOP, considera-se apoiar a J3 nas suas tarefas de controlo e condução das operações, garantindo o contributo de todas as funções militares, asseguradas pelas respectivas células do EMCCOM.

1.3.5 Logística (J4)

Cabe à J4 coordenar e garantir o movimento dos recursos logísticos para dentro, para fora e no interior dos TO, assim como estabelecer as necessárias bases logísticas (NATO AJP-04, 2003). Deve assegurar o correto fornecimento, sustentação e retração das forças no TO, estabelecendo a ligação entre a logística estratégica (proveniente de território nacional/aliado) e a logística no TO (assegurada pelas componentes).

No âmbito da legislação nacional (Decreto-Lei 184, 2014) compete à área dos Recursos, a coordenação e condução dos planos setoriais do movimento e do transporte das FND, assim como acompanhar a sua sustentação, projeção, rotação e retração. É ainda da competência da J4 a coordenação do apoio médico e sanitário às forças na dependência do CEMGFA. Nestas tarefas, o CCOM deve relacionar-se em permanência com os comandos de componente dos ramos.

No âmbito da PCOP, considera-se apoiar a J4 no controlo das diferentes funções logísticas, nomeadamente através da integração do RTLP[20] e na construção de um Panorama Logístico Conjunto[21], que inclua toda a atividade logística, incluindo os Planos Logísticos Estratégicos, PLE (NATO NLH, 2012).

1.3.6 Planos (J5)

À J5 compete, para além da avaliação estratégica militar e da formulação de propostas de opções de resposta militares (MRO)[22], assegurar o planeamento e a coordenação das operações, ao nível operacional e estratégico. Tem a responsabilidade de

[19] recursos e meios
[20] *Recognized Theatre Logistic Picture*
[21] *Joint Logistic Picture*
[22] *Military Response Option*

planear e propor o emprego das forças e meios da COSF, em território nacional e no estrangeiro, incluindo a proposta de Regras de Empenhamento (ROE). Compete-lhe também preparar e atualizar Planos de Operações (OPLAN) e de Contingência (CONPLAN). No âmbito da PCOP, considera-se apoiar a J5 no desenho[23] e planeamento das operações, de forma a construir OPLAN e CONPLAN, sobre base geográfica, capazes de serem utilizado como referência de controlo durante a sua execução.

1.3.7 Comunicações (J6)

À J6 compete o planeamento, aprontamento, implementação, gestão, monitorização e controlo de todas as capacidades de comunicações, bem como dos serviços e sistemas de informação (SI) necessários à satisfação dos requisitos e prioridades de C2, definidos pelo CEMGFA. Deve procurar um controlo centralizado e uma utilização descentralizada dos recursos CIS, assim como assegurar a interoperabilidade dos sistemas que operam dentro da estrutura de comando conjunto (Defesa 2020, 2015) ou combinado (NATO AJP-6, 2011). Caber-lhe-á a implementação e manutenção da infraestrutura de suporte da PCOP, tanto ao nível operacional como na sua ramificação pelas componentes e nível estratégico (em coordenação com a DIRCSI).

1.3.8 Finanças (J7)

A J7 é responsável pela gestão, controlo e operação financeira das operações militares a cargo do CEMGFA. Auxilia na gestão financeira das operações, tendo em conta as leis e regulamentos em vigor. A J7 colabora no planeamento orçamental conjunto das FND e realiza a monitorização dos indicadores estatísticos da atividade desenvolvida. Esta tarefa pode ser apoiada pela PCOP, nomeadamente no controlo financeiro sectorial das unidades e forças destacadas nos TO.

1.3.9 Treino (J8)

A J8 é a célula responsável pela organização, condução e avaliação de exercícios e treino, bem como por recolher e rever análises históricas e lições aprendidas de exercícios e operações anteriores (NATO COPD, 2013). Tem também por missão supervisionar e apoiar as atividades de treino de unidades subordinadas. O registo completo e integrado de toda a atividade desenvolvida no âmbito das operações, e exercícios militares, deve ser feito pela PCOP, para permitir a sua revisão e análise, visando alcançar lições aprendidas,

[23] designado na doutrina inglesa por *Joint Operations Picture* (UK JDP 3-70, 2008)

envolvendo o CTAC.

1.3.10 CIMIC (J9)

A J9 é responsável pela coordenação das atividades que estabelecem e exploram as relações entre as FFAA, o governo, as organizações, as autoridades civis não-governamentais e a população civil no TO (NATO AJP-3.4.9, 2013), tanto numa envolvente amigável, como neutra ou hostil, a fim de facilitar as operações militares, bem como consolidar e atingir os objetivos da missão. Compete ao EMCCOM, nomeadamente à J9, "identificar e planear o emprego das forças e meios afetos à COSF, nas ações de cooperação com as forças e serviços de segurança no combate a agressões ou ameaças transnacionais, bem como em missões de proteção civil" (Decreto-Lei 184, 2014).

2. Identificação dos *stakeholders* da PCOP

As partes interessadas, ou *stakeholders,* constituem as pessoas, grupos e organizações que podem ter interesse no desenvolvimento do projeto, ou serem afetados pelos seus resultados. Os *stakeholders* não partilham necessariamente as mesmas necessidades, ou expectativas, pelo projeto. Podem ser internas ou externas à organização e afetados de forma direta ou indireta, positiva ou negativamente, pelo projeto (PMI, 2013). Integram este grupo: patrocinadores, clientes (externos) ou utilizadores (clientes internos), gestores funcionais, equipas de desenvolvimento, equipas de supervisão, assim como fornecedores[24], subcontratados, entidades governamentais, meios de comunicação, entre outros. A importância da gestão de *stakeholders* é de tal forma relevante que a 5ª edição do PMBOK (PMI, 2013) passou a incluir uma nova área de conhecimento destinada ao *Stakeholder Management*[25].

No âmbito do presente trabalho foram identificadas diferentes entidades, internas e externas às FFAA, que pela sua missão, ou responsabilidades (Tabela 1), devem ser consideradas *stakeholders* no projeto da PCOP (Figura 4).

2.1. Cliente

Constituem os clientes as pessoas, ou organizações (internas ou externas à organização), que vão aprovar, adquirir e utilizar o produto, serviço ou resultado do projeto. O CEMGFA constitui-se como o cliente principal da PCOP, enquanto comandante operacional da COSF e das forças e meios que se constituam na sua dependência.

Devem ser também considerados clientes da PCOP, o CCOM, no apoio ao C2 por parte do CEMGFA, assim como os Comandos Operacionais dos Açores (COA) e da Madeira (COM), cuja missão deriva da responsabilidade CEMGFA nas regiões dos arquipélagos.

Entende-se ainda que a utilização da PCOP deve se alargada aos comandantes de componentes (COMFRI[26], COMNAV, CFT e CA) e órgãos estratégicos com responsabilidades no planeamento e condução de operações sob o comando do CEMGFA (CISMIL).

[24] nos projetos TIC, os fornecedores podem ser de dados, informação, tecnologia ou software.
[25] que inclui a elaboração de um plano estratégico para a comunicação e gestão de *stakeholders.*
[26] Comandante da Força de Reação Imediata

Tabela 1 – Identificação e classificação dos *stakeholders* do projeto.
Escalão (Esc): Po – Político; Es – Estratégico; Op – Operacional; Ta – Tático e Pa – Parceiros.

Unidade / Entidade	Esc.	Sponsor	Cliente / Utilizador	Fornecedor Informação	Equipa do projeto	Direção e Supervisão
DGRDN (MDN)	Po	o				
CEMGFA	Es		**CLIENTE**			
NATO	Es			o		
CISMIL (EMGFA)	Es		o	o		
DIRCSI (EMGFA)	Es					o
EMA (MARINHA)	Es					o
EME (EXÉRCITO)	Es					o
EMFA (FAP)	Es					o
CCOM (EMGFA)	Op		*cliente*	o		o
COA (EMGFA)	Op		*cliente*	o		
COM (EMGFA)	Op		*cliente*	o		
IH (MARINHA)	Op			o	o	
CIGEOE (EXERCITO)	Op			o	o	
CIMFA (FAP)	Op			o		
COMFRI (EMGFA)	Ta		o	o		
COMNAV (MARINHA)	Ta		o	o		
CINAV (MARINHA)	Ta				o	
CFT (EXÉRCITO)	Ta		o	o		
CINAMIL (EXÉRCITO)	Ta				o	
CA (FAP)	Ta		o	o		
CIAFA (FAP)	Ta				o	
DITIC (MARINHA)	Ta				o	
DCSI (EXERCITO)	Ta				o	
DCSI (FAP)	Ta				o	
BTID (PRT)	Pa			o	o	
SIOPS (PRT)	Pa			o		

2.2. **Patrocinador**

O patrocinador, ou *sponsor*, é a pessoa, grupo ou organização, que fornece os recursos e o apoio, necessários para a concretização do projeto (PMI, 2013). Cabe ao *sponsor* financiar o projeto, assim como o promover junto dos decisores de topo da organização e dos *stakeholders*. É responsável pela sua iniciação e pelo seu encerramento. Participa na definição do âmbito do projeto e aprova o seu termo de abertura[27]. Durante a execução, participa nas comissões de acompanhamento, nas revisões dos objetivos e na aprovação das transições de fase e aceitação do produto final. O patrocinador deve também assegurar a transferência harmoniosa dos resultados do projeto para a fase de negócio[28],

[27] autorização formal para se iniciar o projeto.
[28] ou transposição para a fase operacional, quando o projeto é interno à organização.

Constitui-se patrocinador da PCOP a DGRDN[29]. Cabe à DGRDN conceber, desenvolver, coordenar e executar as políticas de recursos humanos, armamento, bens, equipamentos, património, infraestruturas e I&D, necessárias às FFAA e à defesa nacional. Compete-lhe ainda, participar no processo de planeamento de forças e na edificação de capacidades militares, com vista à elaboração das propostas de lei de programação militar; assegurar a execução e o controlo do ciclo de planeamento de defesa; e supervisionar o exercício das atividades de indústria e comércio de bens e tecnologias militares.

2.3. **Gestores Funcionais**

Os gestores funcionais são elementos, ou grupos, chave que detém responsabilidades administrativas, técnicas ou funcionais, dentro da organização e que devem ser incluídas no projeto como elementos da equipa de desenvolvimento, consultores ou fornecedores de informação.

2.3.1. De nível estratégico

O EMGFA constitui o quartel-general das FFAA e integra as estruturas e as capacidades que o CEMGFA necessita no apoio ao exercício das suas competências. Dentro desta estrutura identificam-se como *stakeholders*, com responsabilidades administrativas e técnicas na área do projeto, a DIRCSI e a CISMIL.

A DIRCSI é a entidade nacional com responsabilidade no planeamento, estudo, direção, coordenação e execução dos projetos de sistemas CIS, necessários ao C2 das FFAA. Compete-lhe no âmbito das competências do CEMGFA, em coordenação com o MDN[30], definir os sistemas integrados de Comando, Controlo, e Comunicações (C3), assim como os sistemas CIS, guerra eletrónica e ciberdefesa, a serem operados pelas FFAA. Cabe ainda à DIRCSI, elaborar os requisitos operacionais e técnicos respeitantes aos sistemas C3, considerados nos planos de defesa militar e de contingência, bem como desenhar a sua arquitetura de forma coerente à normalização de equipamentos e à promoção da interoperabilidade sistémica dentro das FFAA e parceiros externos.

O CISMIL tem por missão assegurar a produção de informações necessárias à garantia da segurança militar e ao cumprimento das missões das FFAA, promovendo a produção sistemática de informações de nível estratégico militar no apoio à decisão do CEMGFA. Cabe-lhe ainda produzir informações para a preparação e condução das

[29] Direção Geral de Recursos de Defesa Nacional
[30] Ministério da Defesa Nacional

operações militares, controladas pelo CCOM, incluindo a recolha, processamento e disseminação de informação geoespacial[31].

2.3.2. De nível operacional

Apesar de se constituírem unidades integradas nos ramos, considera-se que tanto o Instituto Hidrográfico (IH), como o Centro de Informação Geográfica do Exército (CIGEOE) e o Centro de Informação Meteorológica da Força Aérea (CIMFA) são organismos técnicos com a capacidade operacional de apoiar todas as componentes militares que se constituam sob o comando do CEMGFA, assim como com a capacidade técnica para integrar a equipa de projeto da PCOP.

O IH é o órgão de Marinha que tem por missão assegurar as atividades de I&D relacionadas com as ciências e as técnicas do mar, tendo em vista a sua aplicação prioritária no apoio, planeamento e execução de operações militares navais. O IH é também laboratório de estado para as áreas da hidrografia, da cartografia náutica, da segurança da navegação e da oceanografia.

O CIGEOE é a unidade do Exército que tem por missão produzir e fornecer informação geográfica ao Exército, FFAA, Forças de Segurança e comunidade civil. Assegura atividades relacionadas com a cartografia e promove a I&D no âmbito da ciência geográfica.

O CIMFA é a unidade da FAP[32] que tem por missão produzir e fornecer informação meteorológica à componente aérea da COSF. A sua capacidade técnica pode ser potenciada no âmbito do projeto, nomeadamente no fornecimento de informação à PCOP.

2.3.3. De nível tático

Constituem unidades com competências funcionais no âmbito do projeto, os comandos de componente de cada um dos três ramos da FFAA, assim como outros que se constituam sob o comando operacional do CEMGFA (PDMC-01, 2012). Estas componentes operam os meios sob o comando do CEMGFA e podem contribuir com os respetivos panoramas táticos (CTP)[33] para alimentar a PCOP.

O CN tem por missão apoiar o CEMA na preparação, aprontamento e sustentação das forças e meios da componente naval da COSF, assim como no seu exercício das

[31] compete também ao CISMIL gerir os Sistemas de Informação Geográfica (SIG) de natureza conjunta.

[32] Força Aérea Portuguesa

[33] *Common Tactical Pictures*

funções de autoridade de controlo operacional de submarinos e coordenador das áreas nacionais de exercício de submarinos.

O CFT tem por missão apoiar o CEME na preparação, aprontamento e sustentação das forças e meios da componente terrestre da COSF.

O CA tem por missão apoiar o CEMFA na preparação, aprontamento e sustentação das forças e meios da componente aérea da COSF, assim como no planeamento e C2 da atividade aérea em território nacional.

Constituem-se ainda gestores funcionais com competências técnicas no âmbito da PCOP, as Direções de Tecnologias de Informação e Comunicações de cada um dos três ramos: DITIC (Marinha); DCSI-E (Exército) e DCSI-FAP (FAP). Estas direções têm por missão assegurar, nos respetivos ramos, o exercício da autoridade técnica nos domínios dos CIS, assim como promover e participar em projetos I&D.

2.4. **Parceiros**

Os parceiros são organizações externas que estabelecem ralações formais com a organização, através de contratos, protocolos ou memorandos de entendimento. Prestam serviços ou fornecem conhecimentos especializados, recursos, equipamentos ou software. No âmbito da PCOP, é importante considerar como *stakeholders* a Industria de Defesa, as Universidades e os Centros de Investigação nacionais (BTID[34]).

2.5. **Outros *stakeholders***

No âmbito do presente trabalho foi possível identificar outros *stakeholders* que importa considerar no desenvolvimento da PCOP, nomeadamente os centros de investigação das três academias militares (CINAV[35], CINAMIL[36] e o CIAFA[37]) como podendo fazer parte da equipa de projeto; os Estados-Maiores dos ramos como entidades de direção e supervisão do projeto; o Sistema Integrado de Operações de Proteção e Socorro (SIOPS[38]) como fornecedor de informação externo às FFAA e a própria NATO.

[34] ver definição (Anexo A)
[35] Centro de investigação Naval
[36] Centro de Investigação, Desenvolvimento e Inovação da Academia Militar
[37] Centro de Investigação da Academia da Força Aérea
[38] ver definição (Anexo A)

2.6. **Organização dos *stakeholders***

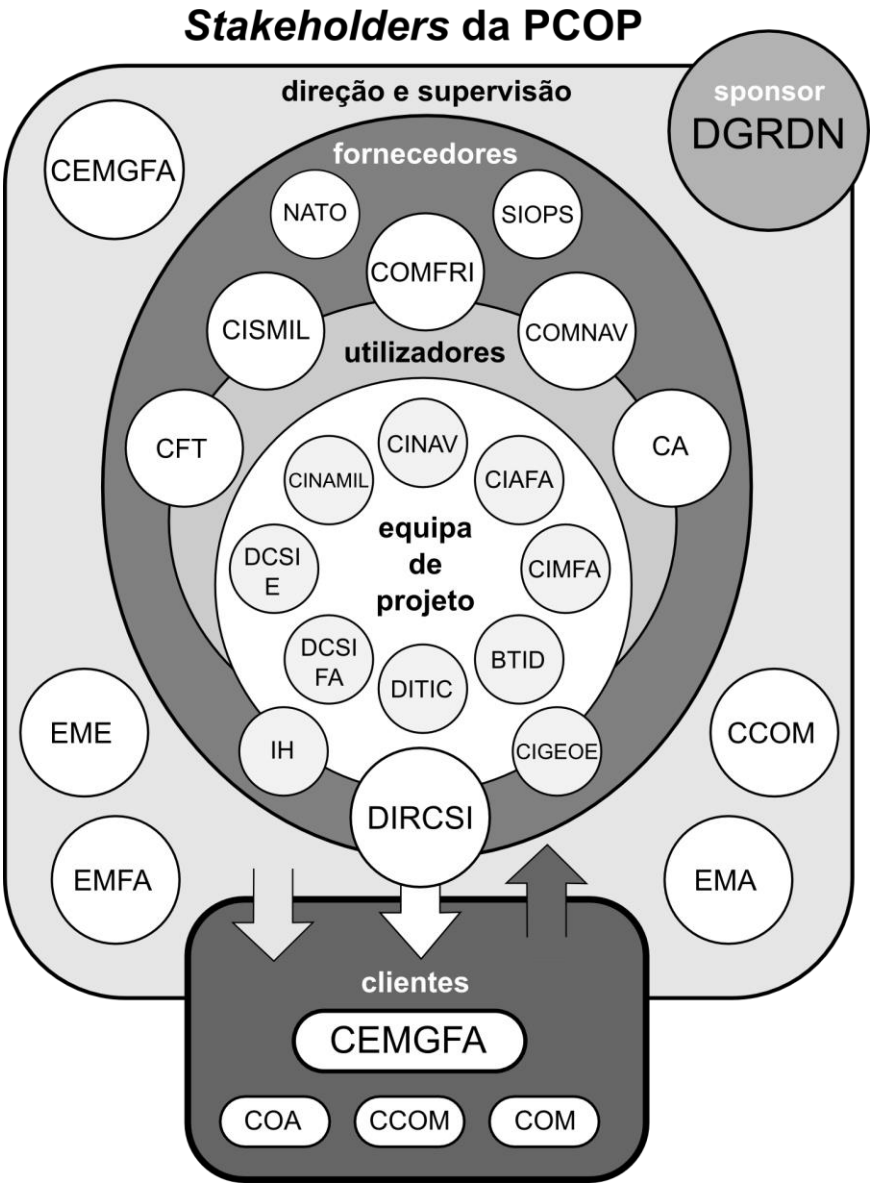

Figura 4 – Organização dos *stakeholders* da PCOP.

Fonte: (autor, 2017)

3. Conceito de Operação da PCOP

No processo de desenvolvimento de *software*, o Conceito de Operação (ConOps[39]) constitui um documento, produzido no início do projeto, onde se antecipam as funcionalidades e o uso pretendido para o novo sistema[40] (Mostashari et al., 2012). O ConOps descreve, do ponto de vista do utilizador, as características, missão, desempenho e necessidades tecnológicas básicas do sistema a desenvolver (IEEE, 1998).

3.1. Definição de COP

O conceito de COP[41] é habitualmente utilizado, num contexto operacional[42], para identificar uma capacidade de integração e visualização de informação georreferenciada, relevante no apoio à decisão. Uma análise da doutrina NATO permite constatar que a definição de COP não é constante nas suas publicações, e muito menos entre outras doutrinas militares de forças aliadas. Esta terminologia só muito recentemente apareceu no Glossário NATO (NATO AAP-06, 2016), apesar ser considerado um requisito operacional de alta prioridade para a Aliança, a disponibilizar a toda a estrutura de comando (Fanti & Beach, 2002). A NATO definiu a COP como uma "imagem operacional, moldada aos requisitos do utilizador e baseada em dados e informação comum, partilhada por mais do que um comando".

Outras doutrinas militares ampliam o conceito de COP. Os ingleses definem a COP como uma imagem operacional comum, capaz de integrar, sobre um mesmo referencial geográfico e temporal, dados correlacionados, analisados e validados, com origem em diferentes CTP (UK JDP 3-70, 2008). Os norte-americanos definem a COP como um sistema capaz de integrar e disponibilizar numa única imagem, informações relevantes, partilhadas pelos diferentes níveis de comando, com a finalidade de criar uma consciência situacional comum e facilitar o planeamento colaborativo (US JP 3-0, 2017). Por fim, é curioso constatar que a Guarda Costeira Norte-Americana designa a COP como um ambiente de trabalho, onde se integram as capacidades de processamento de dados distribuídos, a troca de informação, a partilha de ferramentas de processamento, assim como capacidades de comunicações (US Coastal Guard, 2004).

[39] não confundir ConOp com CONOPs (ver Apêndice 2)
[40] o ConOps deve focar o que a ferramenta fará? e porquê?, sem se preocupar em como?
[41] *Common Operational Picture*
[42] este conceito não é exclusivo às operações militares.

3.2. **Missão da PCOP**

Considera-se, no âmbito do presente trabalho, que a PCOP terá por missão apoiar o planeamento colaborativo, o comando unificado e o controlo das operações militares nacionais conjuntas, através da organização do campo de batalha e da integração, visualização, gestão e partilha de informação relevante, que permita uma compreensão comum e partilhada do ambiente operacional aos diferentes níveis de Comando e Controlo.

3.3. **Gestão do campo de batalha**

Os confrontos militares atuais não reconhecem fronteiras territoriais nem se limitam a conflitos entre nações vizinhas. Os TO são cada vez mais distantes, vastos e complexos, abrangendo diferentes domínios físicos, assim como o domínio virtual[43]. Esta complexidade obriga a uma organização do campo de batalha, definindo áreas de responsabilidade, espaços de interesse, posicionado unidades militares[44], identificando objetivos operacionais e assimilando informações no espaço e no tempo.

3.3.1. Organização do espaço

O campo de batalha moderno compreende diferentes combinações dos domínios mar, terra, ar e espaço, assim como do domínio virtual. Embora estes espaços sejam conceitos úteis para organizar as operações, o uso do termo "domínio" não deve ser interpretado como dimensão dominante, onde prevaleça a exclusividade, primazia ou comando, sobre qualquer outro. De acordo com a doutrina militar podemos descrever o campo de batalha como um agregado de sete domínios/espaços complementares (US JP 3-0, 2017):

a) Domínio marítimo: o mar constitui uma proporção significativa do campo de batalha. Cobre todo o volume submerso, desde o fundo dos oceanos até à sua superfície, margens litorais e mares interiores. É na faixa litoral que ocorrem, atualmente, a maioria das operações militares navais. A superioridade militar é ganha com o controlo do litoral, negando o seu acesso às forças opositoras e permitindo a projeção de poder, fogo, forças e meios aliados em TO terrestres.

b) Domínio terrestre: o espaço terrestre compreende ambientes muito diversificados. Acresce a esta diversidade, o facto dos confrontos militares atuais ocorrerem maioritariamente em ambientes urbanos, muito complexos e dinâmicos. A organização e sincronização das operações desencadeadas neste

[43] domínio da ciberguerra (ciberespaço)
[44] aliadas, neutras e opositoras

domínio torna-se determinante para o sucesso da missão, uma vez que nele podem operar em simultâneo diferentes componente militares (terrestre, anfíbias, aérea e operações especiais), assim como unidades de apoio logístico.

c) Domínio aéreo: o espaço aéreo cobre toda a superfície da Terra, sobrevoando ambos os domínios anteriores. Todas as componentes requerem o acesso ao ar, seja para fazer fogo como para operar aeronaves[45] orgânicas às suas unidades. Este espaço evidencia um elevado potencial de atrito face à sua intensa utilização/ocupação durante as operações militares.

d) Domínio espacial: apesar deste domínio ainda não ser utilizado para operações de combate, ele tem sido ocupado por sistemas de vigilância, comunicações, navegação e meteorologia, no apoio as operações que ocorrem nos restantes domínios.

e) Domínio das informações: a dimensão das informações no campo de batalha, incluindo o ciberespaço, requer uma gestão particularmente ágil para explorar as tecnologias de informação emergentes. Esta deve ser transversal a todas as dimensões e explorada nas manobras de defesa e ataque.

f) Domínio eletromagnético: a dimensão eletromagnética, é finita e encontra-se sob uma pressão cada vez maior devido à proliferação da atividade eletromagnética[46]. Este espaço (espectro electromagnético) pode ser explorado, enquanto fonte significativa de informações, mas é vulnerável face à facilidade de o interromper ou negar.

g) Domínio do tempo: a dimensão tempo é transversal a todas as dimensões. Deve ser explorado para orquestrar atividades e operações militares, através da sincronização e sequenciação. A gestão do tempo deve adotar uma referencia horária comum[47].

3.3.2. Organização das áreas

Na doutrina militar, as áreas operacionais são determinadas consoante a missão atribuída. São definidas por limites geográficos, tempo e âmbito. A geometria do teatro de operações é definida a partir das seguintes áreas:

[45] incluindo *Unmanned Aircraft System* (UAS)
[46] não circunscrito por fronteiras geográficas e disponível para o uso por qualquer componente militar.
[47] nas operações militares utiliza-se frequentemente o fuso "Zulo" (UTC).

Da responsabilidade do nível político-estratégico:

a) Área de Responsabilidade (AOR): atribuída pelo poder político ao comandante estratégico e na qual este é responsável por todas as ações e operações militares;

b) Teatro de Operações (TO): definida pelo comando estratégico e onde a atividade estratégica e operacional podem ocorrer em apoio às operações conjuntas.

c) Área de Operações Conjuntas (JOA): definida pelo comando estratégico e na qual o Comandante de Forças Conjuntas (CTF) ou Combinadas (CJTF) planeia e executa uma missão específica ao nível operacional da guerra. Esta área está incluída dentro do TO e pode contemplar diferentes domínios físicos.

Da responsabilidade do comandante operacional:

d) Área de Operações (AOO): definida pelo CTF para a condução de operações militares específicas, dentro de uma área de operações conjuntas (JOA).

e) Área de Interesse (AOI): definida pelo CTF como área de interesse em relação aos objetivos de operações correntes ou planeados. Esta área inclui as suas áreas de influência, de operações e/ou de responsabilidade, assim como outras áreas adjacentes que importa monitorizar.

Da responsabilidade dos comandantes de componente:

f) Área de Objetivo (OA): área geográfica dentro da qual está localizado um objetivo a ser capturado ou alcançado pelas forças militares. Esta área é definida pela autoridade que detém o C2 destas forças.

g) Área de Influência: área geográfica na qual um comandante é diretamente capaz de influenciar as operações, através da manobra ou de apoio a fogos sob o seu comando ou controlo.

h) Área de Informações (AIR): área atribuída a um comandante e na qual é responsável pela recolha e provisão de informações, utilizando os meios que tem à sua disposição.

3.3.3. Fronteiras

No âmbito militar, as fronteiras separam diferentes áreas de responsabilidade ou de operações distintas. Uma área de responsabilidade não deve ser substancialmente maior que a área de influência do respetivo comandante. As áreas de responsabilidade devem ser exclusivas e os limites não se devem sobrepor. As áreas de responsabilidade podem ser contíguas (pelo menos uma fronteira em comum) ou não-contíguas (sem fronteiras em comum). Se existirem áreas não atribuídas, a responsabilidade pela sua gestão cabe ao escalão superior (US JP 3-0, 2017).

As fronteiras correspondem a espaços de elevado atrito, onde operam diferentes componentes. A extensão destas zonas são definidas frequentemente pelo alcance e a penetração dos sistemas de armas. À medida que o seu tamanho e largura aumentam, também aumenta o grau de complexidade e a necessidade da sua gestão (utilizando para tal sistemas como a COP).

3.4. **Gestão da informação**

De acordo com a doutrina inglesa (UK JDP 3-70, 2008), a COP deu lugar ao conceito JOP[48], definido como o "conjunto total de informações partilhadas sobre uma determinada operação, ou sobre uma JOA, disponível através de um ambiente seguro em redes CIS, para apoiar o CS e as decisão dos comandantes britânicos e facilitar a partilha de informações com aliados e parceiros." Estas informações são integradas sobre um mesmo referencial geográfico e temporal, que tem por base a fusão dos diferentes CTP e panoramas ambientais (REP[49]). A PCOP deve seguir o mesmo conceito, numa base integradora dos diferentes panoramas CS, a disponibilizar pelo CCOM e pelos ramos, assim como pela NATO e outras entidades competentes (Figura 5).

3.4.1. Panoramas Táticos Comuns (CTP)

Os CTP integram numa mesma imagem a posição de meios e unidades aéreas, espaciais, terrestres e marítimas, de modo a construir, em tempo quase-real[50], o CS de cada domínio físico do campo de batalha. Cada elemento[51] é integrado no respetivo panorama e caracterizado por uma posição, grupo-data-hora e classificação. A sua entrada é geralmente feita de forma automática, após detetados por diferentes sensores (ex. radares).

[48] *Joint Operations Picture*
[49] *Recognised Environmental Picture*
[50] atualizados em curtos períodos de tempo (dos micro-segundos na RAP e horas na RMP e RLP)
[51] ex. pessoal, aeronave, navio, carro de combate, antena emissora.

Estas entradas podem ser validadas e limitadas, pelos operadores dos sistemas, aos elementos mais significativos na perspetiva operacional determinada pelo comandante. Esta informação é recolhida nos TO pelos sistemas de armas que integram a maioria das plataformas aéreas e marítimas, bem como por redes de sensores projetados no terreno (ex. radares). Estes sistemas localizam os vários elementos que têm visíveis na sua área de alcance radar. Os seus operadores validam e classificam as entradas e as redes *multi-tactical data link* disponibilizam os panoramas, via rádio ou *web-service*, para outras plataforma ou quartéis-generais.

3.4.1.1. *Recognized Maritime Picture* (RMP)

O RMP é o panorama tático do domínio marítimo. É gerido pelo comandante da componente naval e representa geograficamente o seu CS, nomeadamente a posição e estado operacional das unidades navais da sua força, bem como navios oponentes, neutros e amigos, presentes no TO.

Presentemente, a Marinha partilha a sua RMP (onde estão localizados os meios navais da COSF em operação) com a NATO, através do sistema MCCIS[52]. Este CTP irá brevemente ser substituído pelo sistema TRITON, um projeto I&D da NATO, que pretende construir e disponibilizar um CS marítimo federado, aliado e completo, à escala global, para o qual as nações aliadas partilham a sua RMP e imagem *white-shipping*[53]. A Marinha gere a sua *white-shipping* através da ferramenta OVERSEE[54].

A PCOP deverá garantir os requisitos de segurança e interoperabilidade necessários para partilhar informação com o futuro sistema TRITON.

3.4.1.1. *Recognized Land Picture* (RLP)

O RLP é o panorama tático do domínio terrestre. É gerido pelo comandante da componente terrestre e deve representar geograficamente o seu CS do TO, incluindo a posição das suas forças e localização prevista das unidades militares neutras e opositoras.

Presentemente, o Exercito opera dois sistema C2 que importa considerar no âmbito da PCOP. Ao nível do comando da componente terrestre da COSF, o sistema SICCE tem a capacidade de gerar uma RLP dos meios nacionais projetados nos TO, assim como integrar informação complementar visando a construção de CS do domínio terrestre. Ao nível do

[52] *Maritime Command and Control Information System*
[53] panorama dos navios e plataformas marítimas, não militares.
[54] desenvolvida em parceria com a empresa portuguesa *Critical Software*.

C2 de baixo escalão, o exército está a desenvolver o sistema BMS[55], com as funcionalidades de *Blue Force Tracking*, troca de informação e integração de sensores disponíveis nos CC[56] *Pandur*. Ambos os sistemas poderão constituir fontes de RLP à PCOP, que por sua vez a poderá partilhar com a NATO através do futuro CTP terrestre, o LC2IS[57], em desenvolvimento no seio da Aliança.

3.4.1.1. *Recognized Air Picture* (RAP)

O RAP é o panorama tático do domínio aéreo. É gerido pelo comandante da componente aérea e representa geograficamente o seu CS, nomeadamente o movimento, em tempo real, das aeronaves em movimento sobre o TO.

Presentemente, a FAP partilha a sua RAP[58] com a NATO através do sistema ICC[59]. Este CTP irá brevemente ser substituído pelos sistemas ACCS[60] e AirC2IS[61]. O ACCS constituirá a base do Sistema Integrado de Defesa Aérea e Mísseis da NATO (NATINAMDS) e o AirC2IS será o futuro Sistema Automático de Informação Estratégica (Bi-SC AIS). A PCOP deverá garantir os requisitos de segurança e interoperabilidade necessários para partilhar informação com estes novos CTP, em particular com o AirC2IS.

3.4.1. Partilha de outros Panoramas

A integração dos CTP na PCOP deverá ser complementada com a fusão de outros panoramas, e informação geoespacial, necessária para consolidar um CS completo do TO e contribuir para um C2 eficaz da COSF, por parte do CEMGFA:

a) *Recognized Special Forces Picture* (RSFP): panorama das operações e das informações relacionadas com a atividade e objetivos das SOF.

b) *Recognized Theatre Logistics Picture* (RTLP): panorama das atividade (localização e movimentos) e dados administrativos (recursos, classes e quantidades) de apoio logístico no TO.

c) *Recognised Joint Picture* (RJP): representação dos planos futuros de um CTF ou CJTF, sobre a geometria do campo de batalha previsto.

[55] *Battlefield Management System*
[56] Carros de Combate
[57] *Land Command and Control Information Service*
[58] incluído posição das aeronaves da COSF, em operação, e *white-picture* do tráfego aéreo comercial e privado que sobrevoa o espaço de responsabilidade nacional.
[59] *Integrated Command and Control Software for Air Operations*
[60] *Air Command and Control System*
[61] *Air Command and Control Information System*

d) *Recognised Environmental Picture* (REP): panorama do ambiente geofísico do campo de batalha, obtido a partir da observação, análise e previsão de parâmetros meteorológicos e oceanográficos (METOC), destinado a apoiar a decisão nas fases de planeamento e condução de operações conjuntas, numa área geográfica e momento temporal específico (NATO AAP-06, 2016). A REP pode ser fornecida à PCOP pelo futuro Centro Meteorológico e Oceanográfico Naval (CMETOC), através do serviço METOCMIL[62], em colaboração com o CIMFA e outros produtores de informação METOC.

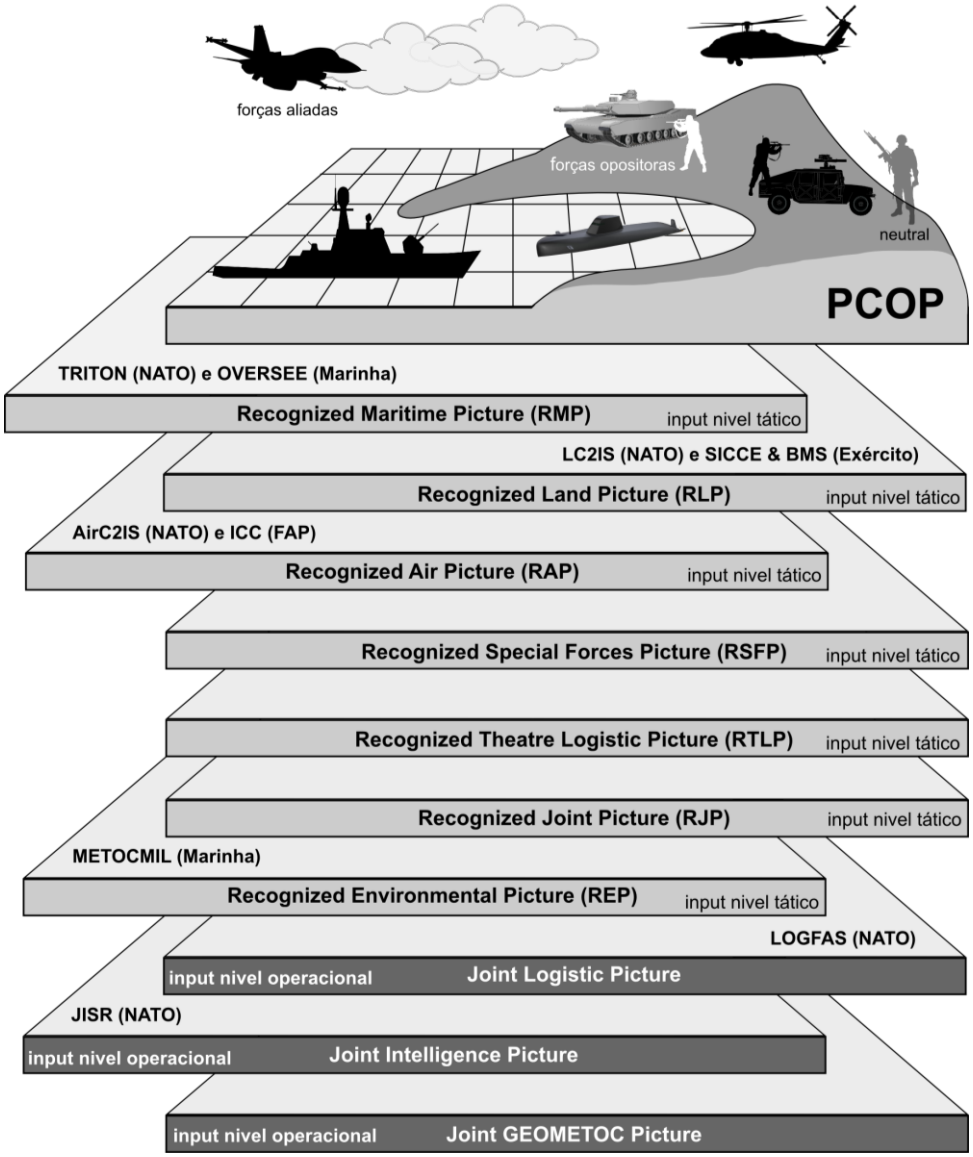

Figura 5 – Representação pictórica da integração da informação na PCOP

Fonte: (autor, 2017)

[62] Meteorologia e Oceanografia Militar

4. Requisitos Críticos da PCOP

Na definição do conceito de uma nova ferramenta é importante realizar um levantamento, e registo, dos requisitos críticos de alto-nível do produto. Estes são determinados pelos seus principais *stakeholders* e estabelecem condições indispensáveis a ter em consideração no desenho e desenvolvimento do produto, constituindo referência no processo de controlo do seu âmbito, a garantir ao longo do ciclo de vida do projeto (PMI, 2013).

4.1. Dados, informação e conhecimento

Os dados são o produto das observações de um sistema e têm uma utilidade relativamente limitada, cingindo-se a um valor quantitativo. O seu valor aparece quando, processados, adquirem valor relacional (qualidade), transformando-se em informação. O conhecimento valoriza a informação e transforma-a em instruções, que permitem o controlo do sistema e a melhoria da sua eficácia. A compreensão pressupõe um nível de conhecimento tal, que possibilite a avaliação e a correção de erros no sistema. Finalmente, a sabedoria corresponde à capacidade de utilizar a compreensão do sistema por forma a deduzir as consequências, a longo prazo, de qualquer ato sobre ele efetuado, assim como prever os seus efeitos na prossecução do estado final desejado (Ackoff, 1989).

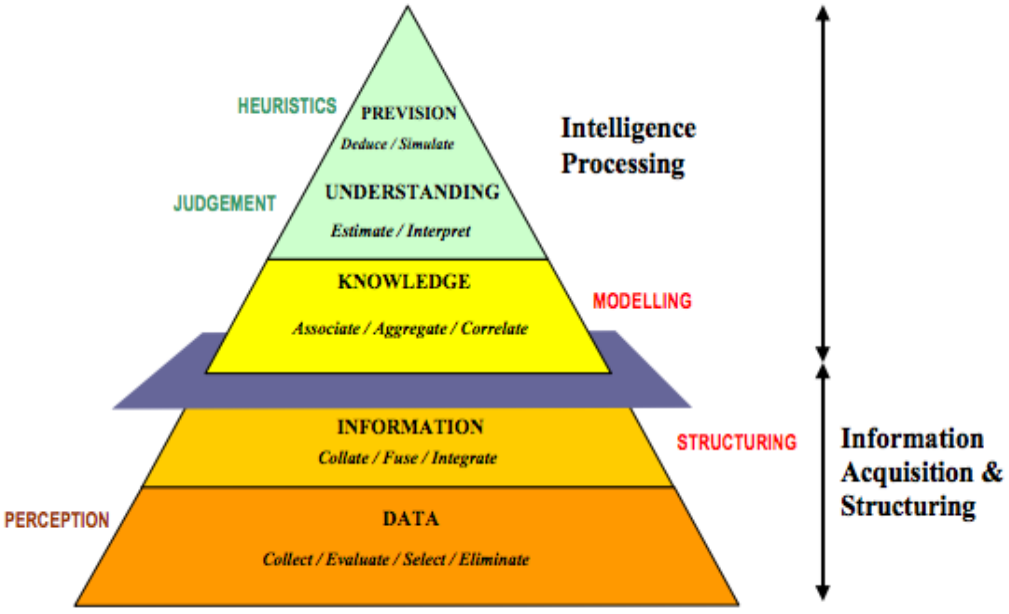

Figura 6 - A pirâmide do "Conhecimento" de Ackoff

Fonte: (Biermann et al., 2004)

A "*pirâmide do conhecimento*" foi recentemente adotada pela NATO (NATO Bi-SC KD, 2011). No contexto militar, este modelo integra os diferentes processos numa cadeia de *Knowledge Development*[63] (KD), partindo dos dados recolhidos no campo de batalha até à sua compreensão efetiva pelo comandante. Abarca os processos de aquisição, análise e distribuição de informação, que contribuem para uma compreensão comum e partilhada do ambiente operacional.

4.2. **Sistemas de Informação e Comunicação**

Segundo a doutrina NATO (NATO AJP-6, 2011) a KD constitui a disciplina que orienta e apoia a utilização da informação, durante todo o seu ciclo de vida, garantindo a sua relevância e disponibilidade no momento certo, e na forma correcta, para satisfazer as necessidades operacionais. Para assegurar um C2 eficaz, é necessário um elevado grau de troca de informação, tanto vertical como horizontal, entre os seus níveis de comando. Constituem ferramentas KD os Sistemas de Comunicações (CS) e os Sistemas de Informação (SI), que no seu conjunto são designados por CIS[64].

4.3. **Requisitos dos CIS**

As FFAA dependem dos CIS para partilhar informação e conhecimento. Esta dependência é de tal maneira crítica que obriga a adoção de um conjunto de princípios e requisitos que garantam a interoperabilidade dos seus sistemas C2, explorando os benefícios da tecnologia e limitando os riscos a ela associados. De acordo com a doutrina NATO (NATO AJP-6, 2011), constituem requisitos críticos dos CIS:

a. Aptidão. Os CIS devem ser definidos pela estrutura de comando e garantir os Requisitos de Partilha de Informação (IER)[65] definidos pelo comandante;

b. Interoperabilidade[66]. C2 de operações conjuntas e combinadas requerem CIS compatíveis entre si, garantido uma troca de efetiva de informação;

c. Agilidade. Os CIS devem responder dinamicamente a operações diversificadas, às mudanças do ambiente operacional ou das necessidades do comando, bem como à escalada do esforço militar, exigência do ritmo de batalha, postura das operações e interrupções na rede;

[63] ver definição (Anexo A)
[64] ver definições (Anexo A)
[65] ver definição (Anexo A)
[66] desenvolvido no Apêndice-C.

d. Segurança. Os CIS devem garantir a segurança da informação, pessoal, meios e infraestruturas, exigida pelos níveis de confidencialidade, integridade, risco e disponibilidade de serviços e SI, definidos para a missão. A segurança da informação deve considerar a capacidade de encriptação[67].

e. Escalabilidade. Os CIS devem ser flexíveis para responder a diferentes necessidades e utilizar um conjunto limitado de recursos. Devem estar preparados para responder às diferentes fases de uma operação militar;

f. Resiliência. Capacidade de recuperação dos sistemas após alterações da sua envolvente ou interrupções indesejadas. É conseguida através da combinação de redundância e robustez, contra eventos acidentais, ou ataques. A Redundância é a capacidade de um sistema em garantir os mesmos serviços a partir de sistemas alternativos, que entram em operação com a falha de sistemas operacionais. Robustez é a capacidade dos sistemas suportarem um determinado nível de "stress", ou exigência do ambiente operacional, sem sofrer degradação, ou perda de funcionalidades;

g. *Service-Oriented*. A integração de diferentes sistemas obriga à adoção de ferramentas adicionais que funcionem como interfaces que garantam a operacionalidade na sua federação. A NATO preconiza a necessidade de pensar os novos SI partindo de requisitos de interoperabilidade, que minimizem a utilização de interfaces e garantam uma federação simplificada e preparada para integrar serviços comuns da Aliança;

h. Autonomia. Capacidade dos CIS em operarem de forma independente da disponibilidade, controlo e influência de outros sistemas externos, bem como de qualquer logística, pessoal ou infraestrutura pré-existente.

i. Prontidão. A tecnologia deve ser selecionada e implementada de forma a garantir os serviços que dela dependem (ex. sistemas de combate, que necessitam de uma resposta imediata; ou serviços de apoio a funções logísticas, que são menos exigentes no tempo de resposta).

[67] ver definição (Anexo A).

4.4. **Requisitos da gestão da informação**

A informação é um recurso organizacional vital. Deve ser gerido, organizado e controlado ao longo de todo o seu ciclo de vida. Numa interpretação direta da política NATO (NATO C-M(2012)0014, 2012) considera-se informação operacional toda aquela que é criada ou recebida no decurso de uma operação e mantida como evidência em cumprimento de obrigações legais. Não existindo doutrina nacional para a gestão da informação operacional, propõem-se, no âmbito dos requisitos da PCOP, considerar os seguintes princípios (NATO AJP-6, 2011):

a. Propriedade da Informação. A informação deve ter associado um originador e claramente definidos os direitos de propriedade, ao longo do seu ciclo de vida.

b. Liderança e Estrutura Organizacional. A gestão da informação requer responsabilidade na sua utilização e disseminação, pelo deve ser organizada de forma estruturada e eficaz, atribuindo a NATO essa responsabilidade aos mais elevados níveis de comando.

c. Partilha da informação. A partilha de informação é fundamental para se alcançar um C2 eficaz. Potencia capacidades e garante a homogeneidade na perceção do ambiente operacional, por parte de todos os níveis de comando e funções militares. Na doutrina NATO, os requisitos de partilha de informação devem ser publicados num COI[68] e detalhados em IER.

d. Normalização da Informação. A informação deve ter estruturas padronizadas e representações consistentes, para permitir a interoperabilidade, a cooperação, a eficiência e eficácia dos processos (NATO APP-6, 2011)

e. Garantia da Informação. A informação e os SI devem ser protegidos de forma a garantir a sua disponibilidade, integridade e confidencialidade: Os sistemas devem garantir o acesso à informação ao pessoal, entidades e sistemas que dela necessitem e que para tal estejam devidamente autorizados (disponibilidade); a informação (incluindo os dados) não podem ser alterados, ou destruídos, de forma não autorizada (integridade); a informação não pode ser disponibilizada ou divulgada a pessoas, entidades ou processos não autorizados (confidencialidade).

[68] ver definição (Anexo A).

Conclusão

O desenvolvimento do conceito de uma *Portuguese Common Operational Picture* (PCOP), teve por principal objetivo identificar as expectativas do CCOM, relativamente à ferramenta a desenvolver, envolvendo e alinhando os *stakeholders* no processo e enquadrando a solução na doutrina militar.

Pretendeu-se, dentro dos parâmetros de um trabalho desta natureza, encontrar um caminho exequível e adequado para suprimir uma lacuna há muito identificada no CCOM: a falta de um SI de apoio à decisão operacional, capaz de apoiar o CEMGFA nas suas competências de C2 da COSF. Pretendeu ainda, numa perspetiva de interoperabilidade entre o EMGFA e os ramos, explorar as capacidades já existentes, de forma a reduzir custos do projeto e a envolver neste desígnio toda a comunidade das FFAA. Esta opção, permitiu criar uma compreensão partilhada das necessidades do CCOM e definir de forma conjunta os critérios de sucesso do projeto.

Os produtos desenvolvidos neste trabalho, pretendem dar visibilidade ao âmbito da PCOP, definir as suas caraterísticas principais e identificar os requisitos críticos a ter em conta no seu desenho e construção. No ciclo de vida dos projetos, estes documentos ajudam a definir a visão do projeto (*o que é necessário fazer?*), a submeter ao seu sponsor (DGRDN) para avaliação e aprovação.

Figura 7 – Representação pictórica do conceito da PCOP.
"combater sobre o mesmo campo de batalha"

Fonte: (autor, 2017)

Em síntese, a PCOP pretende ser uma ferramenta integradora de informação operacional, capaz de organizar o campo de batalha e de disponibilizar, aos diferentes níveis C2, uma imagem de base geográfica, que permita uma compreensão comum e partilhada do ambiente operacional no TO (Figura 7). Esta capacidade visa o planeamento colaborativo, o comando unificado e o controlo das operações militares nacionais conjuntas. Cada utilizador deverá poder filtrar a informação que lhe é relevante para apoiar a sua decisão e contribuir de acordo como as suas funções e área de responsabilidade.

Caberá ao sponsor, na fase que se segue, decidir se este projeto deve ser desenvolvido, repensado ou abandonado.

Referências bibliográficas

(DOD), U.D.o.D., n.d. *DOD Dictionary of Military and Associated Terms*. [*Online*] disponivel em http://www.dtic.mil/doctrine/dod_dictionary [Acedido a 29 Maio de 2017].

Ackoff, R., 1989. From Data to Wisdom. *Journal of Applies Systems Analysis*, 16, pp.03-09.

AIAA, 2011. *Proposed American National Standard: Guide to the Preparation of Operational Concept Documents*. Draft. American Institute of Aeronautics and Astronautics.

Biermann, J. et al., 2004. From Unstructured to Structured Information in Military Intelligence – Some Steps to Improve Information Fusion. In *Symposium on "Systems, Concepts and Integration (SCI) Methods and Technologies for Defence Against Terrorism"*. London, 2004. SCI, NATO RTO.

CEM, 2014. *Conceito Estratégico Militar*. Conselho de Chefes de Estado-Maior, Ministério da Defesa Nacional, Governo de Portugal.

Decreto-Lei 134, 2006. *Cria o Sistema Integrado de Operações de Proteção e Socorro (SIOPS) (com as alterações introduzidas pelo Decreto-Lei nº 114/2011)*. D.R. 1ª Série nº142, de 25 de Julho.

Decreto-Lei 184, 2014. *Lei orgânica do Estado-Maior-General das Forças Armadas (EMGFA)*. D.R. 1ª Série nº250 de 29 de dezembro.

Decreto-Lei nº1-A, 2009. *Lei Orgânica de Bases da Organização das Forças Armadas (LOBOFA)*. D.R. 1.ª série, N.º 129 de 7 de Julho.

Defesa 2020, 2015. *Reforma estrutural da Defesa Nacional e das Forças Armadas*. Ministério da Defesa Nacional, Governo de Portugal.

Fanti, L. & Beach, D., 2002. NATO initial common operational picture capability project. In *Battlespace Digitization and Network-Centric Warfare II*., 2002. SPIE.

IEEE, 1998. *Guide for Information Technology — System Definition — Concept of Operations (ConOps) Document*. Software Engineering Standards Committee of the IEEE Computer Society, IEEE, Genebra.

INCOSE, 2012. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities, version 3.2.2. San Diego, CA, USA: International Council on Systems Engineering (INCOSE)*.

ISO/IEC/IEEE, 2015. *Systems ans Software Engineering — System Life Cycle Processes (ISO/IEC/IEEE 15288)*. Genebra, Suiça: International Organisation for Standardisation / International Electrotechnical Commissions, Institute of Electrical and Electronics Engineers.

ISO/IEC, 2008. *Systems and software engineering -- System life cycle processes (ISO/IEC 15288)*. International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC), ISO/IEC JTC 1/SC 7.

IUM, 2015. *NEP / ACA - 010 Trabalhos de Investigação*. Instituto de Estudos Superiores Militares (EMGFA).

Joint Vision 2020, 2000. *America's Military - Preparing for Tomorrow*. Washington DC: Chiefs of Staff.

Mostashari, A. et al., 2012. Developing a Stakeholder-Assisted Agile CONOPS Development Process. *Systems Engineering*, 15, pp.1-13.

NATO AAP-06, 2016. *NATO Glossary of Terms and Definitions (English and French)*. NATO Standardization Office (NSO).

NATO AAP-39, 2015. *Handbook of Land Operations Terminology (B)*. NATO Standardization Office (NSO).

NATO AJP-04, 2003. *Alled Joint Logistic Doctrine (A)*. NATO Standardization Agency (NSA).

NATO AJP-3.4.9, 2013. *Allied Joint Doctrine for Civil-military Cooperation*. NATO Standardization Agency (NSA).

NATO AJP-6, 2011. *Allied Joint Doctrine for Communication and Information Systems*. NATO Standardization Agency (NSA).

NATO APP-6, 2011. *NATO Joint Military Symbology (C)*. NATO Standardization Agency (NSA).

NATO ATP 3.2.2, 2016. *Command and Control of Allied Land Forces (B)*. NATO Standardization Office (NSO).

NATO Bi-SC KD, 2011. *Bi-Strategic Command Knowledge Development (Pre-Doctrinal Handbook)*.

NATO C-M(2012)0014, 2012. *Directive on the Management of Records Generated on Operational Deployment*. NATO Military Committee.

NATO COPD, 2013. *Allied Command Operations Comprehensive Operations Planning Directive (COPD)*. 2nd ed. Bélgica: NATO Supreme Headquarters Allied Powers Europe.

NATO NLH, 2012. *NATO Logistics Handbook*. NATO Logistics Committee, NATO Graphics & Printing.

Paul, R. & Elder, L., 2006. *The Miniature Guide to Critical Thinking - Concepts and Tools*. The Foundation for Critical Thinking.

PDMC-01, 2012. *Doutrina Nacional conjunta*. EMGFA, Ministério da Defesa Nacional, Governo de Portugal.

PMI, 2013. *PMBOK - A Guide to the Project Management Body of Knowledge*. 5th ed. Atlanta, USA: Project Management Institute ed.

Sisney, L., 2012. *Organizational Physics - The Science of Growing a Business*. Santa Barbara: organizationalphysics.com, Elaine Johnson ed.

UK JDP 3-70, 2008. *Battlespace Management*. Development, Concepts and Doctrine Centre.

UK JSP 777, 2005. *Network Enabled Capability*. Ministry of Defence UK, Joint Service, Publication.

US Coastal Guard, 2004. *Standard Operating Procedures for the Common Tactical and Common Operational Picture*. Homeland Security Digital Library.

US JP 2-0, 2013. *Joint Intelligence*. US Joint Chiefs of Staff, US Department of Defense (DOD).

US JP 3-0, 2017. *Joint Operations*. US Joint Chiefs of Staff, US Department of Defense (DOD).

ANEXOS e APENDICES

Anexo A — Definição de conceitos

Base Tecnológica e Industrial para a Defesa (BTID): conjunto das empresas e entidades do Sistema Científico e Tecnológico Nacional (SCTN[69]), públicas ou privadas, com capacidade para intervir numa ou mais etapas do ciclo de vida dos equipamentos e sistemas utilizados pela Defesa. A estratégia de desenvolvimento da BTID resulta de uma iniciativa conjunta entre o Ministério da Defesa Nacional e o Ministério da Economia, de forma a desenvolver a Industria Nacional de Defesa, considerando-a um valor estratégico para o desenvolvimento económico e segurança do país.

Capacidade Militar: De acordo como (CEM, 2014), constitui o "conjunto de elementos que se articulam de forma harmoniosa e complementar e que contribuem para a realização de um conjunto de tarefas operacionais ou efeito que é necessário atingir, englobando componentes de doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade, entre outras (DOTMLPII)".

Community of Interest (COI): Documento que define os níveis e cargos com interesse por determinada informação, no apoio às funções e atividades operacionais (NATO AJP-6, 2011)

Conhecimento Situacional (CS): conhecimento necessário dos elementos do campo de batalha para apoiar as tomadas de decisão CITATION AAP16 \l 2070 (NATO AAP-06, 2016)

Encriptação: ferramentas, hardware e/ou software, que constituem um serviço de suporte à confidencialidade, integridade e disponibilidade das informações partilhadas entre sistemas (NATO AJP-6, 2011).

Information Exchange Requirements (IER): Definem a necessidade de troca de informações entre duas ou mais partes que apoiam um determinado processo, enfatizando o princípio de segurança de "necessidade de conhecimento", da reutilização e da não-duplicação da informação. Descrevem a fonte e o destino do fluxo de informações, o conteúdo, assim como o formato, a classificação de segurança, a capacidade de fluxo, requisitos de desempenho e atributos de conteúdo e contexto (NATO AJP-6, 2011)

Knowledge Development (KD): processo contínuo, adaptativo e em rede, de formação de conhecimento, realizado aos diferentes níveis do comando (estratégico, operacional e tático). Fornece aos comandantes, e ao seu *staff*, uma compreensão

[69] ver definição (Anexo A)

abrangente de ambientes complexos, incluindo as relações entre os sistemas e os atores, dentro do campo de batalha (NATO COPD, 2013).

Sistema Integrado de Operações de Proteção e Socorro (SIOPS) constitui o conjunto de estruturas, normas e procedimentos que asseguram a coordenação de todos os agentes de proteção civil, atuando no plano operacional, articuladamente sob um comando único, sem prejuízo da respetiva dependência hierárquica e funcional. O SIOPS constitui um importante stakeholder para o projeto PCOP, nomeadamente como fornecedor de informação no apoio às operações CIMIC (Decreto-Lei 134, 2006).

Sistemas de Comunicações (CS): Constituem os equipamentos, métodos, procedimentos e, se necessário, o pessoal especializado e organizado para realizar funções de transferência de informação (NATO AAP-06, 2016).

Sistemas de Informação (SI): Constituem os equipamentos, métodos, procedimentos e, se necessário, o pessoal especializado e organizado para realizar funções de processamento de informação (NATO AAP-06, 2016). O desenvolvimento, utilização e emprego destas ferramentas deve seguir um Plano de Gestão da Informação, de forma a alcançar uma partilha efetiva e adequada, entre as forças, os comandos de componente e o comandante operacional. Este plano deve selecionar, organizar e dirigir, a informação, os CIS necessários para constituir a rede federada, os Requisitos de Partilha de Informação (IER[70]) assim como os requisitos de segurança da informação. da Aliança.

Sistema Científico e Tecnológico Nacional (SCTN): constitui o conjunto dos recursos institucionais, humanos, financeiros e informacionais, assim como dos projetos e das atividades organizadas para a produção cientifica e tecnológica em Portugal. Constitui uma capacidade estratégica nacional, traduzida no conhecimento, investigação e inovação de base científica, fomentando a sua transferência e aplicação para a industria, a fim de se alcançarem os objetivos do desenvolvimento cientifico, económico, cultural e social.

[70] *Information Exchange Requirements*.

Apêndice A — Ciclo de vida do desenvolvimento de uma ferramenta

O desenvolvimento de uma nova ferramenta COP constitui um Processo de Engenharia de Sistemas, segundo o qual a construção, ou adaptação, de um sistema deve ter em consideração o seu ciclo de vida, da iniciação ao estado final e terminado no seu abate. Este ciclo é definido de forma distinta por diferentes normas internacionais[71].

A norma ISO/IEC 15288 padroniza internacionalmente uma coleção de processos que constituem o ciclo de vida dos sistemas, com base em princípios e conceitos que regem a sua aplicação. A norma foi construída de modo a poder ser aplicada a qualquer tipo de sistema artificial (ISO/IEC, 2008)

Cada sistema tem um ciclo de vida. Este ciclo pode ser descrito a partir de um modelo funcional abstrato que integre as diferentes fases da vida do sistema. Cada fase tem um propósito e uma contribuição distinta para o desenvolvimento, operação, manutenção e abate do sistema. Cada uma destas fases deve ser considerada em todo o processo de planeamento e desenvolvimento do sistema. Um sistema evolui ao longo destas fases, em resultado de ações organizadas, realizadas segundo processos capazes de avaliar o seu desempenho. Entre cada fase existem pontos de decisão (ou condições decisivas) que permitem aos decisores, da organização, determinar a conclusão da respetiva fase e consequente transposição para a fase seguinte. Estes pontos de decisão são usados para controlar as incertezas inerentes ao projeto de desenvolvimento e aos riscos associados a custos, cronograma, recursos e âmbito previstos no plano de projeto. O detalhe dos modelos que traduzem o ciclo de vida de um sistema é expresso em termos de processos, fases, resultados, relações e pontos de decisão.

Tabela 2 - Fases do ciclo de vida dos sistemas, respectivos objectivos e tomadas de decisão em cada ponto de transição de fase, tal como definido na norma ISO/IEC 15288

LIFE CYCLE STAGES	PURPOSE	DECISION GATES
CONCEPT	Identify stakeholders' needs Explore concepts Propose feasible solutions	Decision Options: - Execute next stage - Continue this stage - Go to previous stage - Hold project activity - Terminate project
DEVELOPMENT	Refine system requirements Create solution description Build system Verify and validate system	
PRODUCTION	Mass produce system Inspect and test	
UTILIZATION	Operate system to satisfy users' needs	
SUPPORT	Provide sustained system capability	
RETIREMENT	Store, archive or dispose the system	

Fonte: (ISO/IEC, 2008)

[71] Como são exemplos o standard IEEE 1220-2005 e o ISO/IEC 15288-2008

A tabela 2 apresenta as principais fase do ciclo de vida do sistema, tal como definidas na ISO/IEC 15288. A norma foi definida para constituir uma base comum e universal à organização dos ciclos de vida dos sistemas, mas deixou liberdade às organizações para adaptarem as fases e processos do ciclo às suas estratégia empresariais (frequentemente contrastantes relativamente aos modelos de negócio, recursos disponíveis, oportunidades de tecnologia e modelos de mitigação de riscos).

Embora a norma ISO/IEC 15288 não exija, nem defenda um modelo de ciclo de vida específico, existem vários modelos documentados que foram sendo construídos e adotados pela industria de desenvolvimento de software e hardware. O modelo "Vee" (INCOSE, 2012) constitui uma referência amplamente utilizada. Este modelo traduz, com uma representação gráfica na forma da letra "V", o ciclo de desenvolvimento de sistemas, sintetizando as suas principais fases, processos e resultados (Figura 8). As fases dispõem-se sequencialmente ao longo do tempo e sobrepõem-se por três períodos distintos do ciclo: período de definição, de implementação e integração. Do lado esquerdo do modelo estão representadas as etapas que devem definir as especificações do sistema e levantar os seus requisitos. O vértice da letra "V" representa a fase de construção ou implementação do sistema. Do lado direito do modelo estão representas as etapas de teste, validação e integração do sistema no ambiente operacional.

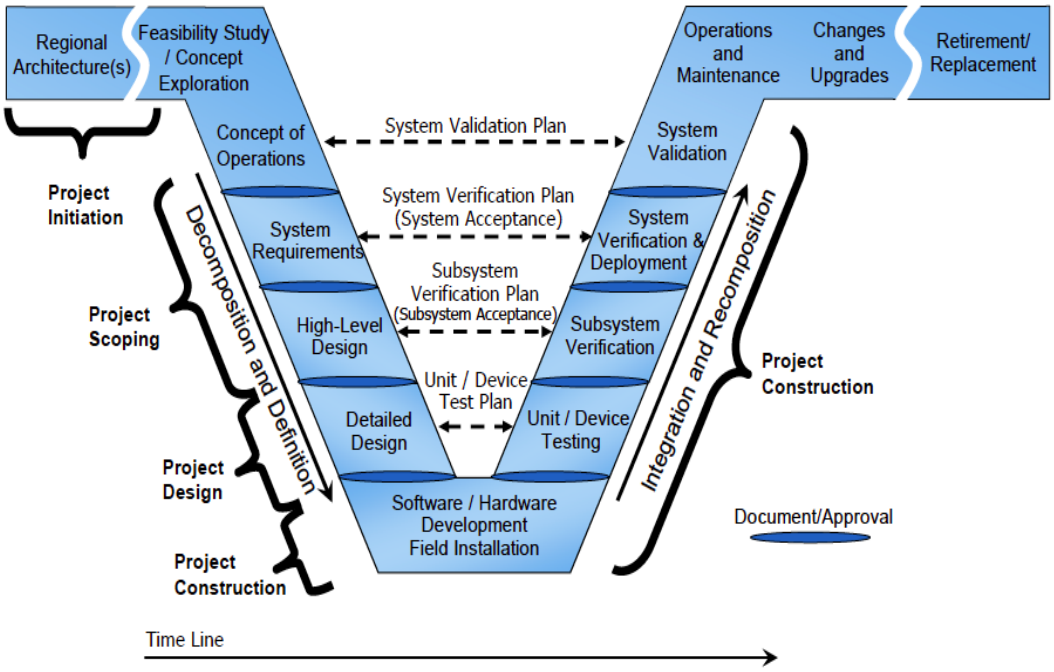

Figura 8 - Fases do ciclo de vida dos sistemas, respectivos outputs e dependências inter-fase, como desenhado no modelo "Vee".

Fonte: (INCOSE, 2012)

De acordo com a norma ISO/IEC 15288, a fase conceptual constitui a primeira etapa do ciclo de vida de um sistema. Tem por missão avaliar novas oportunidades de negócio e desenvolver requisitos preliminares de novos sistemas e avaliação da viabilidade do seu projeto de desenvolvimento (ISO/IEC, 2008)

Esta fase começa com o reconhecimento inicial de uma necessidade ou de um conceito para um sistema novo, ou modificação de sistema já existente. Trata-se de uma pesquisa inicial, onde se recolhem factos junto das partes interessadas (clientes/mercado) e se constrói um conceito com base no *feedback* do cliente/usuário. São desenvolvidas uma ou mais soluções alternativas para dar resposta à necessidade, ou conceito identificado. São realizadas análises, avaliações de viabilidade, estimativas (tais como custo, cronograma, inteligência de mercado e logística), estudos de trade-off e desenvolvimento experimental de protótipo e demonstração.

Os produtos desta fase, de acordo como a ISO/IEC 15288, são: os requisitos das partes interessadas, o conceito de operação, os requisitos preliminares dos sistemas, as soluções de projeto na forma de esboços, desenhos, modelos ou protótipos e a avaliação da sua viabilidade. Nesta fase podem ser identificadas outras necessidades de desenvolvimento (ex. novos sistemas facilitadores), podem ser estimados custos acumulados ao logo do ciclo de vida do sistema, assim como previstos os recursos humanos requeridos para o desenvolvimento do projeto e operação do sistema. Esta informação, em conjunto com cronogramas preliminares de desenvolvimento do projeto permitirão aos decisores tomar partido pela continuação do mesmo (dando inicio à fase de desenvolvimento) ou pelo cancelamento do projeto.

Apêndice B — Conceito de Operações vs Conceito de Operação

Os termos "Conceito de Operação" e "Conceito de Operações", são frequentemente utilizados indistintamente no âmbito do desenvolvimento de projetos. Apesar de existirem semelhanças entre estes dois conceitos, a sua definição e âmbito são distintos:

a. **Conceito de Operações (CONOPS).** Modelo abstrato criado por uma organização para descrever como pretende operar para atingir as suas metas e objetivos. O conceito de operações pode ser de nível estratégico e independente dos sistemas particulares a serem utilizados na organização, ou pode ser desenvolvido como parte do processo de aquisição de um novo sistema (AIAA, 2011). Apresentam-se aqui três definições diferentes de CONOPS:

   i. NATO glossary of terms and definitions, (NATO AAP-06, 2016): O CONOPS é uma "declaração clara e concisa da linha de ação escolhida por um comandante para realizar sua missão".

   ii. Dictionary of Military and Associated Terms ((DOD), n.d.): O CONOPS é uma "declaração verbal ou gráfica que expressa clara e concisamente o que o comandante da força conjunta pretende realizar e como o vai realizar utilizando os recursos disponíveis. O conceito é utilizado para dar uma visão geral da operação".

   iii. INCOSE Systems Engineering Handbook, (INCOSE, 2012): O ConOps constitui um documento "produzido no início do processo de definição de requisitos para capturar uma compreensão livre de implementação das necessidades das partes interessadas, definindo o que é necessário, sem abordar como satisfazer a necessidade. Deve capturar as características comportamentais exigidas do sistema, no contexto de outros sistemas com os quais interage e capturar a maneira como as pessoas interagem com o sistema para o qual o sistema deve fornecer capacidades. Pode também definir quaisquer requisitos críticos de desempenho de nível superior ou os objetivos (declarados qualitativa ou quantitativamente) e a racionalidade do sistema".

b. **Conceito Operacional (OpsCon).** Declaração verbal e gráfica dos pressupostos, ou intenções, de uma empresa em relação à operação, ou série de operações, a realizar por um sistema, ou conjunto de sistemas, em desenvolvimento (AIAA, 2011). O conceito operacional é frequentemente desenvolvido como parte de um programa de desenvolvimento ou aquisição de sistemas. É desenhado para traduzir a forma de funcionamento do sistema na perspetiva do operador/utilizador e ser a base para a definição de requisitos do sistema. O conceito Operacional é definido num documento designado frequentemente por OpsCon.

Apêndice C — Interoperabilidade dos sistemas CIS na NATO

A interoperabilidade é definida pela NATO como a capacidade de atuação conjunta, coerente, eficaz e eficiente para alcançar objetivos táticos, operacionais e estratégicos (NATO AAP-06, 2016). A interoperabilidade dos sistemas, é definida como a capacidade dos sistemas em fornecer informação e serviços a outros sistemas, e vice-versa (NATO AJP-6, 2011). Para alcançar este fim, devem ser estabelecidos requisitos que garantam a integração, total ou parcial, dos CIS aos diferentes níveis de comando, possibilitando assim um C2 eficaz de forças conjuntas e combinadas.

A doutrina NATO define três tipos de interoperabilidade (NATO AJP-6, 2011):

a. Sintática - Alcançada quando dois ou mais sistemas cumprem os mesmos protocolos de comunicação, formatos de mensagem e dados, para suportar a troca de dados;

b. Estrutural - Alcançada quando dois ou mais sistemas são simultaneamente sintáticos e concordam em comunicar para produzir e/ou consumir dados, numa troca estruturada com o mesmo arranjo de informação e granularidade[72].

c. Semântica - Alcançada quando dois ou mais sistemas, são simultaneamente estruturais e têm a capacidade de interpretar automaticamente as informações trocadas de forma significativa e precisa para produzir resultados úteis, conforme definidos pelos utilizadores.

A interoperabilidade não é uma condição absoluta na NATO. É extremamente difícil uniformizar o desenho dos sistemas desenvolvidos por cada país aliado, assim como os seus requisitos de segurança nacional. Para ultrapassar estas circunstâncias, a NATO estabelece diferentes níveis de interoperabilidade entre sistemas aliados, segundo os quais se estabelecem redes comuns de sistemas federados na Aliança (NATO AJP-6, 2011):

a. Nível 0 - Interoperabilidade isolada. Os sistemas são isolados uns dos outros e requerem intervenção humana para fornecer interoperabilidade, através de *gateways* manuais (ex. *memory stick, hard disk*)

[72] Granularidade diz respeito ao nível de detalhe ou de resumo contido nos pacotes de dados partilhados ou armazenados nas bases de dados. Quanto maior o nível de detalhes, menor o nível de granularidade. Afeta diretamente a velocidade de troca de dados e o volume de dados armazenados.

b. Nível 1 - Interoperabilidade ponto-a-ponto. Os sistemas são fisicamente ligados por ligação eletrónica, proporcionando uma interação direta entre si (voz modulada em frequência, *links* táticos e e-mail). Os produtos dos sistemas devem ser homogéneos de forma a possibilitar a sua partilha. Os dados são separados das aplicações.

c. Nível 2 - Interoperabilidade Funcional (Ambiente distribuído). Aplicações independentes tem a capacidade de trocar e usar dados e componentes de dados independentes, de forma direta ou distribuída entre os sistemas (troca de imagens ou mapas anotados)

d. Nível 3 - Interoperabilidade de Domínio (Ambiente Integrado). Os sistemas estão integrados num mesmo domínio, que inclui modelos de dados e procedimentos de partilha entre aplicações independentes (que podem trabalhar em conjunto de forma integrada). Enquanto que os dados são armazenados em bancos de dados partilhados, os aplicativos ainda estão separados dos dados (ex. COP partilhada).

e. Nível 4 - Interoperabilidade Empresarial (Ambiente Universal). Os dados são totalmente partilhados entre aplicativos que trabalham juntos em domínios de acesso comum. A colaboração entre usuários é muito avançada (ex. COP interativa).

A interoperabilidade entre dois CIS pode alcançada através de:

a. Normas Técnicas. São conjuntos de regras que permitem estabelecer configurações ou procedimentos operacionais apropriados para a troca de informação entre sistemas. Estas normas surgem definidas na conceção, compra ou emprego de novos equipamentos.

b. Gateways. São interfaces de sistemas que resolvem os problemas de interoperabilidade técnica ou processual. Existem dois tipos: Gateways de Interface Técnica, que alteram a natureza dos dados de modo a torná-los permutável entre diferentes sistemas; Gateways de Partilha de Informações, que ligam diferentes domínios de segurança, a fim de verificar e filtrar as informações que podem ser trocadas entre os sistemas.