**INSTITUTO UNIVERSITÁRIO MILITAR**

**DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS**

**CURSO DE ESTADO-MAIOR CONJUNTO**

**2016 / 2017**

**TII**

# O CONTRIBUTO DAS OPERAÇÕES DE INFORMAÇÃO PARA A SUPERIORIDADE DE INFORMAÇÃO

**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.**

**João Paulo Catrola Martins**

**Maj Art**


# INSTITUTO UNIVERSITÁRIO MILITAR

# DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

# O CONTRIBUTO DAS OPERAÇÕES DE INFORMAÇÃO PARA A SUPERIORIDADE DE INFORMAÇÃO

**Maj Art João Paulo Catrola Martins**

Trabalho de Investigação Individual do CEM-C

Pedrouços 2017


# INSTITUTO UNIVERSITÁRIO MILITAR
# DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

# O CONTRIBUTO DAS OPERAÇÕES DE INFORMAÇÃO PARA A SUPERIORIDADE DE INFORMAÇÃO

**Maj Art João Paulo Catrola Martins**

Trabalho de Investigação Individual do CEM-C

Orientador: Maj Art Nelson José Mendes Rego

Pedrouços 2017

**Declaração de compromisso Antiplágio**

Eu, **João Paulo Catrola Martins**, declaro por minha honra que o documento intitulado **O Contributo das Operações de Informação para a Superioridade de Informação**, corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **Curso de Estado-Maior Conjunto 2016/2017** 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, 24 de Julho de 2017

João Paulo Catrola Martins

Maj Art

**Agradecimentos**

Concluído este estudo, quero deixar um especial agradecimentos a todos os que comigo colaboraram para a sua elaboração. A sua disponibilidade em muito contribuiu para o sucesso deste estudo e para alcançar os seus objetivos.

As primeiras palavras vão indubitavelmente para os entrevistados, o Exmº Coronel de Transmissões Paulo Viegas Nunes, professor de outras andanças e mentor de outros tempos, que me despertou o interesse pelo estudo do emprego da informação no espectro da conflitualidade. O outro entrevistado, o LTC Lars Koreman do Exército Alemão e a prestar serviço no *Joint Force Command Brunssum* (JFCBS), agradeço a disponibilidade de tempo, a visão que me deu do funcionamento da Secção de InfoOps do JFCBS e por ter partilhado o seu conhecimento sobre o emprego das InfoOps. *Sir, without your contribution, this essay would not have been possible. My sincere, thank you*.

Não podia deixar de agradecer ao meu orientador, Major de Artilharia Nelson Rêgo. Não só pela orientação, mas especialmente, pela exigência no cumprimento dos prazos. Fez com que não perdesse a orientação e o foco no trabalho. Ser orientador de pelo menos dois discentes, e sobre assuntos tão dispersos, não é tarefa fácil. Para além disso, sempre houve as aulas e outros afazeres.

Outro agradecimento especial, vai para os meus camaradas. Não tenho um feitio fácil, e todos eles sempre souberam lidar com isso.

Por fim, agradeço à família e aos amigos. Não só o apoio, mas pela compreensão das ausências motivadas pelas longas horas de trabalho. Família e amigos não cobram, compreendem e estão sempre lá para apoiar. Assim foi.

**Índice**

**Índice de Anexos**



**Índice de Apêndices**



**Índice de Figuras**

**Índice de Tabelas**

## Resumo

Recorrendo a uma investigação bibliográfica assente na doutrina conjunta da *North Atlantic Treaty Organization* (NATO), a fontes bibliográficas sobre a temática da Guerra Centrada em Rede, Superioridade de Informação (SupInfo) e Operações de Informação (InfoOps) e a entrevistas semiestruturadas com elementos que desempenham funções relativas às InfoOps nos Comandos Conjuntos da NATO, este estudo de caso procura analisar a capacidade militar edificada ao nível Operacional para planear, coordenar e integrar o emprego das capacidades e técnicas das InfoOps e de que modo esta capacidade contribui para que o Comando Conjunto atinja a SupInfo.

Ao longo deste estudo, descreve-se o conceito de SupInfo, como se atinge e quais as condições que a materializam. Seguidamente, é descrito o conceito de InfoOps e qual o produto das capacidades e técnicas integradas por esta função. Por fim, é analisada a capacidade militar edificada na NATO ao nível Operacional, recorrendo para isso ao modelo DOTMLPII. É também analisado o contributo desta capacidade para a materialização das condições para obter a SupInfo.

**Palavras Chave:**

InfoOps, NATO, Superioridade, Informação, Operacional

***Abstract***

Through bibliographic research based on NATO joint doctrine, bibliographical sources on the theme of Network-Centered Warfare, Information Superiority and Information Operations, and through semi-structured interviews with elements that perform functions related to InfoOps in NATO Joint Force Commands, this case study aims to analyse the military capability at the operational level that plans, coordinates and integrates the use of InfoOps capabilities and techniques, and how it contributes to achievement of the condition of Information Superiority by the Joint Force Command.

We start by describing the Information Superiority concept, how it is achieved and what are the conditions that define it. Next, we describe the concept of Information Operations and ascertain what is the product of the capabilities and techniques integrated by this function. Finally, using the DOTMLPII model, the military capability built in NATO at the Operational level and its contribution to materialize the conditions to obtain the Information Superiority is analysed.

**Key Words:**

InfoOps, NATO, Superiority, Information, Operational

**Lista de abreviaturas, siglas e acrónimos**

| | |
|---|---|
| **A** | |
| AA | Audiências Alvo |
| AI | Atividades de Informação |
| AInfo | Ambiente de Informação |
| AJP | *Allied Joint Publication* |
| AO | Área de Operações |
| **C** | |
| C2 | Comando e Controlo |
| C2W | *Command and Control Warfare* (Guerra de Comando e Controlo) |
| C4ISR | *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance* (Comando, Controlo, Comunicações, Computadores, Informações, Vigilância, Reconhecimento) |
| CCOM | Comando Conjunto para as Operações Militares |
| CCRP | *Command and Control Research Program* |
| CEM | Curso de Estado Maior |
| CIMIC | *Civil Military Cooperation* (Cooperação Civil Militar) |
| CME | Contra Medidas Eletrónicas |
| CNA | *Computer Network Attack* (Ataque a Redes de Computadores) |
| CND | *Computer Network Defence* (Defesa das Redes de Computadores) |
| CNE | *Computer Network Exploitation* (Exploração de Redes de Computadores) |
| COPD | *Comprehensive Operations Planning Directive* |
| CyberOps | *Cyberspace Operations* (Operações no Ciberespaço) |
| **D** | |
| DoD | *Department of Defence* |
| **E** | |
| EM | Estado-Maior |
| EMGFA | Estado Maior General das Forças Armadas |
| EUA | Estados Unidos da América |
| **F** | |
| FFAA | Forças Armadas |
| FMN | *Federated Mission Network* |

**G**

| | |
|---|---|
| GCR | Guerra Centrada em Rede |
| GE | Guerra Eletrónica |
| GI | Guerra de Informação |
| GIC | Gestão de Informação e do Conhecimento |

**I**

| | |
|---|---|
| IACB | *Information Activities Coordination Board* |
| InfoOps | *Information Operations* (Operações de Informação) |

**J**

| | |
|---|---|
| JCB/WG | *Joint Coordination Board / Working Group* |
| JFC | *Joint Force Command* (Comando de Forças Conjunto) |
| JFCBS | *Joint Force Command Brunssum* |
| JOPG | *Joint Operational Planning Group* |
| JTCB/WG | *Joint Targeting Coordination Board / Working Group* |

**M**

| | |
|---|---|
| MAE | Medidas de Apoio Eletrónico |
| MoD | *Ministry of Defence* (Ministério da Defesa) |
| MoE | Medidas de Eficácia |
| MPE | Medidas de Proteção Eletrónicas |

**N**

| | |
|---|---|
| NAC | *North Atlantic Council* (Concelho do Atlântico Norte) |
| NATO | *North Atlantic Treaty Organization* (Organização do Tratado do Atlântico Norte) |
| NATO IORH | *Bi-SC NATO Info Ops Reference Handbook* |
| NEP | Normas de Execução Permanente |
| NIOC | NATO *School Information Operations Course* |
| NSOIOC | NATO *Senior Officer Information Operations Course* |

**O**

| | |
|---|---|
| OBE | Operações Baseadas em Efeitos |
| OCR | Operações Centradas em Rede |
| OE | Objetivo Específico |
| OG | Objetivo Geral |

| | |
|---|---|
| OLPP | *Operational Level Planning Process* (PPNO - Processo de Planeamento de Nível Operacional) |
| OODA | Observar, Orientar, Decidir, Agir |
| OPSEC | *Operation Security* (Segurança das Operações) |
| **P** | |
| PA | *Public Affairs* (Informação Pública) |
| PPP | Postura, Presença e Perfil |
| PSYOPS | *Psychological Operations* (Operações Psicológicas) |
| **Q** | |
| QC | Questão Central |
| QD | Questão Derivada |
| **S** | |
| StratCom | *Strategic Communication* – Comunicação Estratégica |
| SupInfo | Superioridade de Informação |
| **T** | |
| TI | Tecnologias de Informação |
| TIC | Tecnologias de Informação e Comunicação |
| TII | Trabalho de Investigação Individual |
| **U** | |
| UK | *United Kingdom* |

## Introdução

Quando se fala em informação e na sua relação com as operações militares, não podemos deixar de falar em Alvin e Heidi Toffler. As suas obras, "A Terceira Vaga" (1980) e "Guerra e Antiguerra" (1993) lançam as fundações para se começar a debater a utilização da informação nas operações militares. Na sua essência, as sociedades conduzem a guerra do mesmo modo que produzem a sua riqueza (Toffler e Toffler, 1994). Vivemos hoje naquela a que designamos por Era da Informação.

Associado ao conceito, surge a ideia de Guerra de Informação (GI), que se entende como sendo as operações conduzidas no domínio da informação. De igual modo, associado ao conceito de informação, está o de rede. A informação circula em redes assentes nas Tecnologias de Informação e Comunicação (TIC).

Importa para esse efeito perceber a forma como as organizações militares utilizam as novas tecnologias e potenciam o funcionamento em rede, e de que modo a sua cadeia de valor é influenciada, condicionando decisivamente a sua atuação e o espaço estratégico em que podem intervir.

Constituindo o funcionamento em rede e a exploração intensiva dos recursos de informação uma condição essencial ao funcionamento das modernas sociedades e das Forças Armadas Portuguesas, pretende-se, através de uma atuação sincronizada no domínio da informação, potenciar a Capacidade de Comando e Controlo (C2) e garantir, de forma eficaz, a operação e defesa das redes de Comunicações e Sistemas de Informação.

Por tudo isto, é necessário compreender como se deve organizar uma estrutura que permita coordenar as diferentes atividades no domínio da Informação garantindo a coerência do seu planeamento e a execução sincronizada das ações a desenvolver, contribuindo assim para assegurar a SupInfo.

Pretende-se que este estudo venha a definir as bases para a edificação de uma estrutura de Estado-Maior (EM) com a capacidade de planear, coordenar e integrar as Operações Militares no domínio da informação. A nível nacional, o Comando Conjunto para as Operações Militares (CCOM) do Estado Maior General das Forças Armadas (EMGFA) é a organização equivalente aos *Joint Force Commands* (JFC) da NATO. Presentemente, este Comando, não dispõe de uma estrutura permanente que planeie, coordene e integre o emprego das InfoOps ao nível Operacional, de forças e contingentes em operações de âmbito militar nos planos externo e interno, pelo que se revela pertinente, pensar sobre o desenvolvimento de uma capacidade semelhante neste Comando.

No âmbito das InfoOps, pretende-se estudar a capacidade militar edificada ao nível

Operacional que permite planear, coordenar e integrar as capacidades e técnicas associadas às InfoOps e de que modo essa capacidade contribui para a obtenção da SupInfo ao nível Operacional.

No que se refere ao objeto, o estudo é delimitado à estrutura de EM de nível Operacional da NATO com responsabilidade de planeamento de InfoOps. Em termos temporais vamos delimitar a investigação às capacidades edificadas a partir de 2012, ano em que a estrutura de comando da NATO sofreu uma profunda alteração, tendo sido adotada a estrutura vigente (NATO, 2013c). Este período engloba também a data da última restruturação do EMGFA (CM, 2014). Em termos espaciais vamos delimitar a investigação ao órgão da estrutura permanente de comando da NATO, JFCBS.

Este estudo tem como objetivo geral (OG) de investigação: No quadro das InfoOps, analisar a capacidade militar edificada ao nível Operacional para planear, coordenar e integrar o emprego das capacidades e técnicas das InfoOps e de que modo contribui para a atingir a SupInfo.

Em suporte a este, foram identificados cinco objetivos específicos (OE) que permitirão atingir o OG. São eles:

OE1: Descrever a cadeia de valor das Operações Centradas em Rede (OCR).

OE2: Descrever como se atinge a SupInfo.

OE3: Descrever o conceito de InfoOps e qual o produto das suas Capacidades e Técnicas.

OE4: Identificar a Capacidade Militar ao nível Operacional que permite planear, coordenar e integrar as diferentes capacidades de InfoOps.

OE5: Compreender como a capacidade militar analisada contribui para a superioridade da informação.

O problema de investigação será resolvido com a resposta à questão central (QC) identificada: Qual a capacidade militar edificada ao nível Operacional para planear, coordenar e integrar o emprego capacidades e técnicas das InfoOps e de que modo contribui para a atingir a SupInfo?

À semelhança do objetivo de investigação, foram identificadas questões derivadas (QD) que nos ajudarão a responder à QC. São elas:

QD1: Qual é o valor acrescentado de se conduzirem OCR?

QD2: Como se atinge a SupInfo?

QD3: Qual é o produto das capacidade e técnicas das InfoOps?

QD4: Existe uma capacidade militar ao nível Operacional que permite planear,

coordenar e integrar as diferentes capacidades de InfoOps?

QD5: Como é que a capacidade militar analisada contribui para a SupInfo?

Para nos auxiliar a responder às QD4 e QD5, recorremos às seguintes hipóteses:

H4.1: A capacidade militar analisada está organizada segundo os vetores de desenvolvimento de uma capacidade militar;

H5.1: A capacidade militar analisada permite satisfazer as condições necessárias para se atingir a SupInfo.

A investigação seguiu uma orientação Epistemológica Interpretivista, tendo sido adotada uma estratégia de investigação qualitativa utilizando para isso um raciocínio indutivo, assente no estudo de caso da Secção de InfoOps do JFCBS.

O estudo está organizado em uma introdução, quatro capítulos e as conclusões. No capítulo um, será efetuada a revisão da literatura e a definição da base conceptual que sustenta o estudo, bem como a descrição do modelo de análise e do percurso metodológico adotado.

No capítulo dois, iremos abordar o caminho para a SupInfo. Faremos uma descrição das OCR, da Cadeia de Valor das OCR, do Ciclo de Decisão e por fim, descreveremos como se atinge a SupInfo e definindo quais as condições que a materializam.

No capítulo três, será efetuada a caracterização da função militar conjunta InfoOps, descrevendo as suas áreas de atividade e as suas capacidades e técnicas. Descreveremos de igual modo como as InfoOps se organizam e integram ao nível Operacional e determinar qual o seu produto para as áreas interrelacionadas e para a finalidade das InfoOps.

No capítulo quatro, será descrita a estrutura de planeamento, coordenação e integração de InfoOps ao nível Operacional. Esta descrição será feita em função dos vetores de edificação de uma capacidade militar. Seguidamente, será analisado de que modo esta estrutura contribui para que o Comando a que pertence, contribui para materializar uma condição de SupInfo sobre um adversário.

Por fim, serão tecidas as conclusões e elaboradas as propostas que se entenderem pertinentes.

Para a elaboração deste estudo, recorreu-se à ferramenta de referenciação bibliográfica Zotero[1].

[1] https://www.zotero.org/

# 1. Enquadramento Conceptual e Modelo de Análise

## 1.1. Estado da Arte

À *priori* do conceito e dos estudos sobre SupInfo, deve-se analisar o conceito que lhe deu origem. A Guerra Centrada em Rede (GCR) foi alvo de estudo inicialmente pelo Almirante Cebrousky e por Garstka no seu artigo de 1998 "*Network-Centric Warfare - Its Origin and Future*". O Departamento de Defesa (DoD) dos Estados Unidos da América (EUA) financia o *Command and Control Research Program* (CCRP) para desenvolver a temática da GCR e estudar as suas implicações para as operações militares. É deste programa que se desenvolve a base da literatura relacionada com esta temática. Alberts, Garstka, Stein, Haeys, editam obras como "*NETWORK CENTRIC WARFARE: Developing and Leveraging Information Superiority*" (1999), "*Understanding Information Age Warfare*" (2001), "*Power to the Edge: Command and Control in the Information Age*" (2003), "*Understanding Command and Control*" (2006), entre outras e onde apresentam os conceitos de SupInfo e para se compreender a GCR, que, entretanto, se passou a designar por OCR.

Em termos nacionais o conceito de GI é abordado pelo Coronel José Dinis (2005) na sua obra "*Guerra de Informação: Perspetivas de Segurança e Competitividade*". Nesta obra, Dinis, caracteriza a sociedade centrada em rede, a GI, faz uma prospetiva futura para a sociedade da informação e sobre as implicações destes conceitos para a temática de Segurança e Defesa. O Tenente Coronel, João Vicente (2007) em "*Guerra em Rede:Portugal e a Transformação da NATO*" analisa a temática da GCR e as suas implicações para as Forças Armadas (FFAA) nacionais. O Coronel Paulo Nunes no seu livro "*Sociedade em Rede, Ciberespaço e Guerra de Informação: Contributos para o Enquadramento e Construção de uma Estratégia Nacional de Informação*" de 2015, propõe, tal como o nome indica, a criação de uma estratégia para o domínio da Informação por parte do Estado Português. A obra conceptualiza de igual modo, a GI e os conceitos de SupInfo que, segundo o autor, são essenciais para se definir uma Estratégia Nacional da Informação.

O conceito de InfoOps está no presente momento, perfeitamente definido na doutrina militar conjunta da NATO. Na revisão de dezembro de 2015 da publicação doutrinária conjunta, "AJP-3.10 *Allied Joint Doctrine for Information Operations*", a Aliança define o que entende por InfoOps e conceptualiza o seu emprego em apoio às Operações Militares Conjuntas, ao nível Estratégico e Operacional.

Academicamente, os estudos mais recentes sobre a temática das InfoOps, OCR e SupInfo, pertencem ao Tenente-Coronel Vítor Lopes em 2008 com o seu Trabalho de Investigação Individual (TII) elaborado durante o Curso de Estado-Maior Conjunto (CEMC)

"*Network Centric Warfare*: Desenvolvimento e Implementação a Nível Nacional". O Major Luís Morais em 2012, no seu TII "As Operações de Informação e a sua implementação nas Forças Armadas Portuguesas" propõe uma solução de implementação de uma estrutura de InfoOps nas FFAA Portuguesas. No entanto este estudo foi realizado não tendo em conta a atual estrutura de comando da NATO[2] e numa época em que as FFAA Portuguesas ainda não dispunham de uma estrutura de Comando equivalente aos JFC da NATO como é o caso do CCOM.

Outros artigos que conceptualizam a temática são o elaborado pelo Tenente-Coronel Carlos Ribeiro "Guerra Centrada em Rede: Um conceito operacional emergente no Século XXI" (2008) publicado na *Proelium*, e o artigo do Coronel Navegador António Eugénio "A Guerra Centrada em Rede: Um breve balanço dez anos depois" (2008), publicado na Revista Militar.

### 1.2. Corpo de Conceitos

Por forma a enquadrar conceptualmente o tema em análise, torna-se necessário definir um conjunto de conceitos, que dada a sua relevância estruturante, serão objeto de referência ao longo do estudo.

#### 1.2.1. Informação

A NATO (2015a, p.2.I.4) define informação como sendo, "*dados genéricos não processados que podem ser utilizados para produzir Informações*". Sendo esta definição muito orientada para o contexto do ciclo de produção de informações, complementa-se a mesma com a definição de Paulo Nunes (2015c, p.34), Informação é "*o conjunto de dados em contexto, cuja forma e conteúdo são apropriados para uma determinada utilização particular, a partir dos quais é possível conhecer um determinado aspeto ou parte da realidade.*".

#### 1.2.2. Superioridade de Informação

Foram Alberts, Garstka e Stein (1999, p.34), quem primeiro definiu SupInfo como sendo, "*o estado que se atinge quando se consegue obter uma vantagem competitiva que advém da capacidade de explorar uma posição informacional superior*".

Para a NATO (2015c) SupInfo é *"... a vantagem operacional que advém da capacidade de recolher, processar e disseminar um fluxo ininterrupto de informação enquanto se explora ou nega a capacidade a um adversário de fazer o mesmo*".

Considera-se de igual modo relevante explanar o conceito à luz da doutrina Inglesa

[2] Implementada em 2012.

(UK MoD, 2013, p.1–1), que considera SupInfo "*…a vantagem competitiva que se ganha através da utilização, continua, dirigida e adaptativa das capacidades, comportamentos e princípios relevantes da informação*".

### 1.2.3. Operações Centradas em Rede

Podemos definir as OCR como: "*…um conceito de operações, resultante da obtenção da SupInfo, que gera um maior poder de combate a partir da integração em rede de sensores, decisores e atiradores para obter uma perceção partilhada, uma maior rapidez da ação de comando, um melhor tempo das operações, maior letalidade, melhor capacidade de sobrevivência,… e um determinado grau de auto-sincronização.*" (Perry et al 2002, cit. por Nunes, 2015a)

### 1.2.4. Capacidade Militar

O conceito de capacidade militar está definido em despacho ministerial, entendendo-se como tal "*o conjunto de elementos que se articulam de forma harmoniosa e complementar e que contribuem para 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*" (MDN, 2014).

São vetores de desenvolvimento de uma capacidade a doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade[3]. O mesmo despacho enuncia áreas de capacidades, são elas: Comando e Controlo; Emprego da Força; Proteção e Sobrevivência; Mobilidade e Projeção; Conhecimento Situacional; Sustentação; Autoridade, Responsabilidade, Apoio e Cooperação.

### 1.2.5. Operações de Informação

Segundo a NATO, (2015b, p.1.5) na sua publicação doutrinária conjunta AJP 3-10, InfoOps é *"…uma função de Estado-Maior (EM) para analisar, planear, avaliar e integrar as atividades no domínio da Informação, de modo a criar os efeitos4 desejados na Vontade, na Compreensão e na Capacidade de potenciais adversários e nas Audiências Alvo (AA) aprovadas pelo NAC*[5] *em apoio aos objetivos da Aliança.*"

Compreendem três áreas interrelacionadas: preservar e proteger a liberdade de ação da Aliança; os comportamentos, perceções e atitudes das AA aprovadas pelo NAC; Contrariar a propaganda adversária e as suas funcionalidades e capacidades de C2 (NATO, 2015b, p.1.6). Já as capacidades e técnicas das InfoOps são: Operações Psicológicas (PSYOPS),

[3] Por norma e doravante referidos por DOTMLPII.
[4] Apêndice B
[5] O *North Atlantic Council* (NAC) é o principal órgão de decisão politica da Aliança Atlântica (NATO, 2016).

Guerra Eletrónica (GE), Operações no Ciberespaço[6] (CyberOps), Presença Postura e Perfil (PPP), Deceção, Segurança das Operações (OPSEC), *Engagement*, Destruição Física, Segurança da Informação (INFOSEC), Relações Publicas (RP) e Cooperação Civil Militar (CIMIC) (NATO, 2015b, p.1.10-1.16).

### 1.3. Modelo de Análise

Nesta investigação, o corpo de conceitos foi obtido através de um quadro de análise que tem como finalidade recolher os elementos que permitam analisar a capacidade militar edificada ao nível Operacional para planear, coordenar e integrar o emprego das capacidades e técnicas das InfoOps e de que modo contribui para a SupInfo.

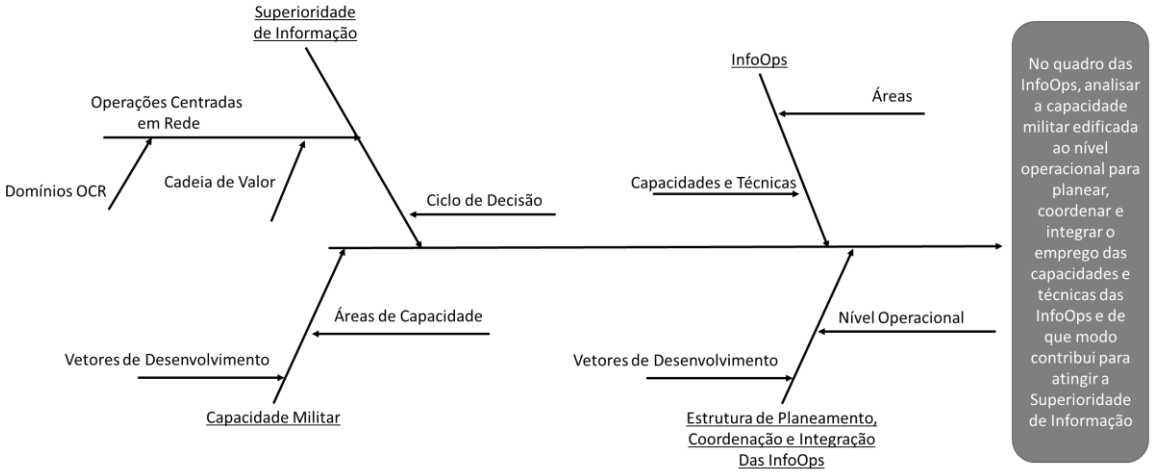



**Figura 1 - Corpo de conceitos**

**Fonte**: Autor (2016b)

O estudo foi conduzido segundo três dimensões de análise. Inicialmente, foi analisado o conceito de SupInfo de modo a poder compreender quais são os requisitos para e como é atingida. Seguidamente foram analisadas as capacidades e técnicas das InfoOps, para se compreender o modo como se operacionalizam as InfoOps ao nível Operacional. Por fim, foi analisada a capacidade militar edificada ao nível Operacional que permite planear, coordenar e integrar as diferentes capacidades e técnicas das InfoOps. Esta análise foi efetuada face às dimensões de análise que correspondem aos vetores de desenvolvimento de uma capacidade militar (DOTMLPII). A relação entre os OE de investigação e as QD, pode ser analisado na Figura 2, abaixo e na Tabela 4 do Apêndice A.

[6] CiberOps são compostas por *Computer Network Attack* (CNA), *Computer Network Exploitation* (CNE) e *Computer Network Defence* (CND).

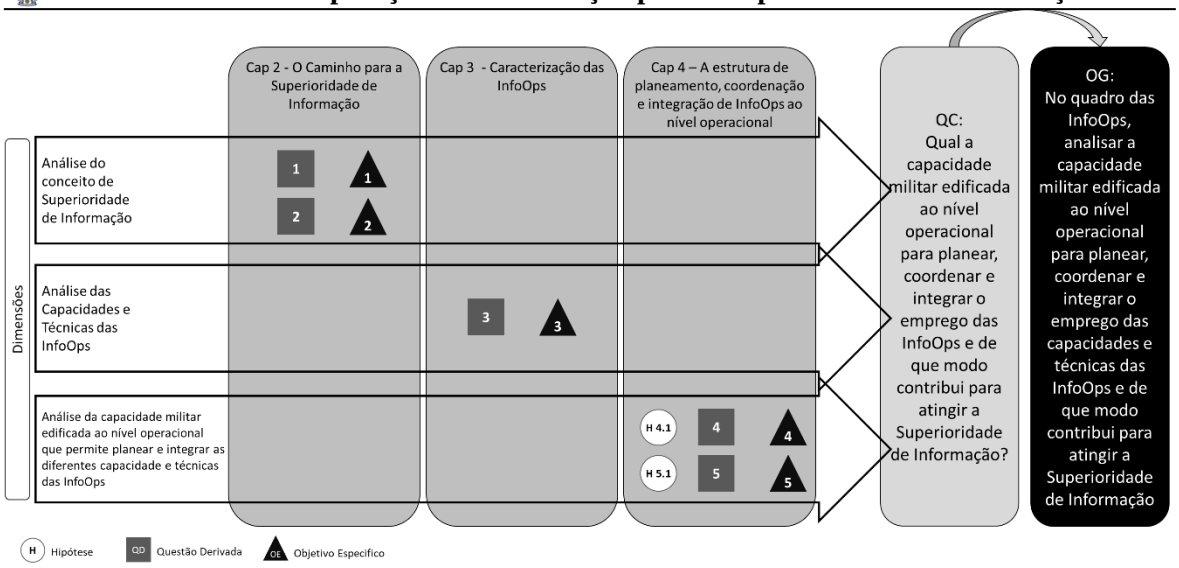



**Figura 2 - Plano geral da investigação**

**Fonte**: Autor (2016d)

### 1.3.1. Resumo da metodologia

A investigação seguiu uma orientação Epistemológica Interpretivista, em que foi adotada uma estratégia de investigação qualitativa recorrendo para isso a um raciocínio indutivo assente num desenho de pesquisa de Estudo de Caso que analisa a estrutura de planeamento, coordenação e integração das InfoOps do JFCBS.

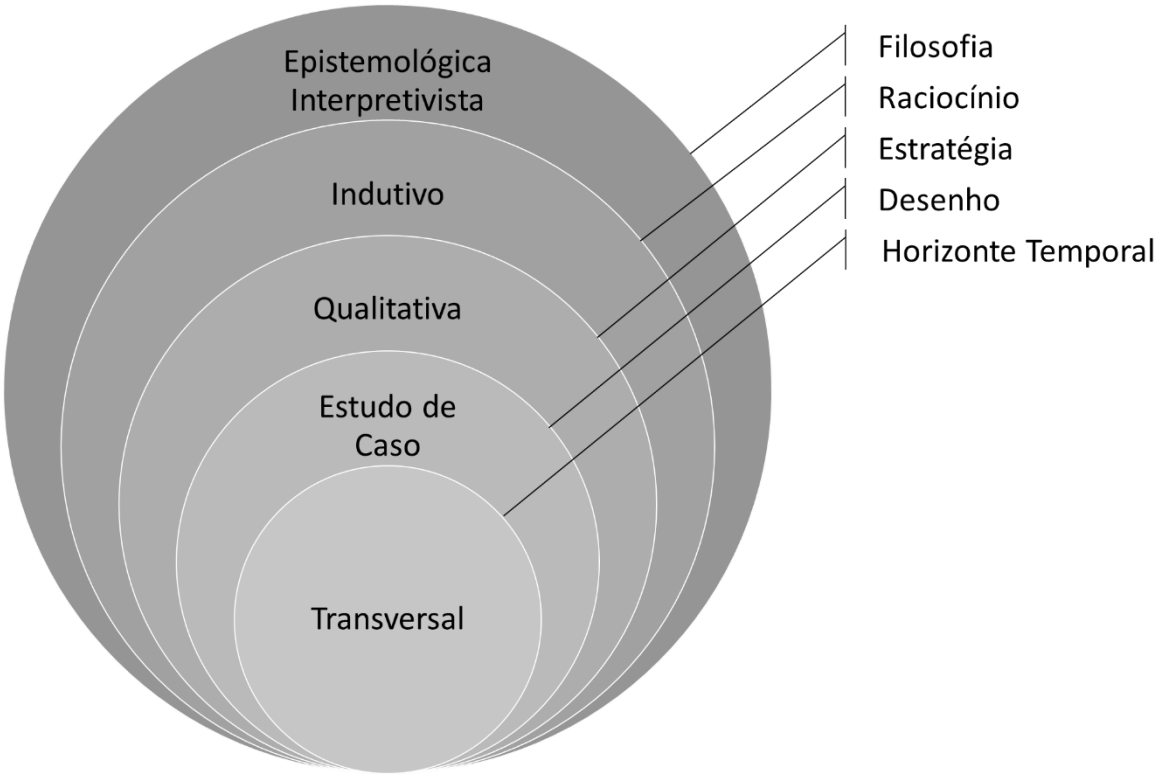



**Figura 3 - A "Cebola" da Investigação**

**Fonte**: Adaptado de Saunders et al. 2009, p108; Autor (2016a)

### 1.3.2. Percurso metodológico

#### 1.3.2.1. Fase exploratória

Esta fase iniciou-se com a escolha do tema por sorteio de entre os temas disponíveis para escolha, tendo culminado com a elaboração de um plano de trabalho. Na definição do estado da arte, procurou-se fazer um levantamento dos conceitos mais atuais de SupInfo, de InfoOps e de capacidade militar. Esta revisão permitiu assim definir o OG da investigação a partir do qual se identificaram cinco OE. Destes, decorreu uma QC que se pretendeu ver respondida com as cinco QD identificadas. A partir daqui, criou-se o modelo de análise. Definiram-se as dimensões de análise e como seriam respondidas as QD que por sua vez permitiriam atingir os QE da investigação.

#### 1.3.2.2. Fase analítica

Durante esta fase procedeu-se ao aprofundamento da revisão da literatura de modo a fundamentar os conceitos estruturantes da investigação. Foi executada a recolha de dados que assentou na revisão bibliográfica doutrinária e conduta de entrevistas. Os dados foram analisados de modo a identificar como estão articulados os vetores de desenvolvimento da capacidade militar (DOTMLPII) para planear, coordenar e integrar as InfoOps ao nível Operacional e a fundamentar o contributo da capacidade analisada para a SupInfo.

A interpretação dos resultados foi feita por análise de conteúdo temática e de relações. As hipóteses foram validadas segundo o conjunto de indicadores que se apresentam na Tabela 5 do Apêndice A.

#### 1.3.2.3. Fase conclusiva

Na fase conclusiva foram apresentados os resultados da investigação.

De um modo gráfico, o percurso metodológico adotado é explicado na Figura 4, abaixo.

### 1.3.1. Instrumentos metodológicos

A investigação assentou essencialmente na consulta de fontes bibliográficas secundárias existente sobre a temática, nomeadamente doutrina conjunta da NATO, EUA, Nacional e outras publicações de referência na temática das OCR, da SupInfo e InfoOps e em documentação interna do JFCBS. Adicionalmente, recorreu-se à recolha de dados de fontes primárias através de entrevistas semiestruturadas a entidades militares que desempenham ou tenham desempenhado cargos relacionados com as InfoOps na estrutura de comando da NATO.

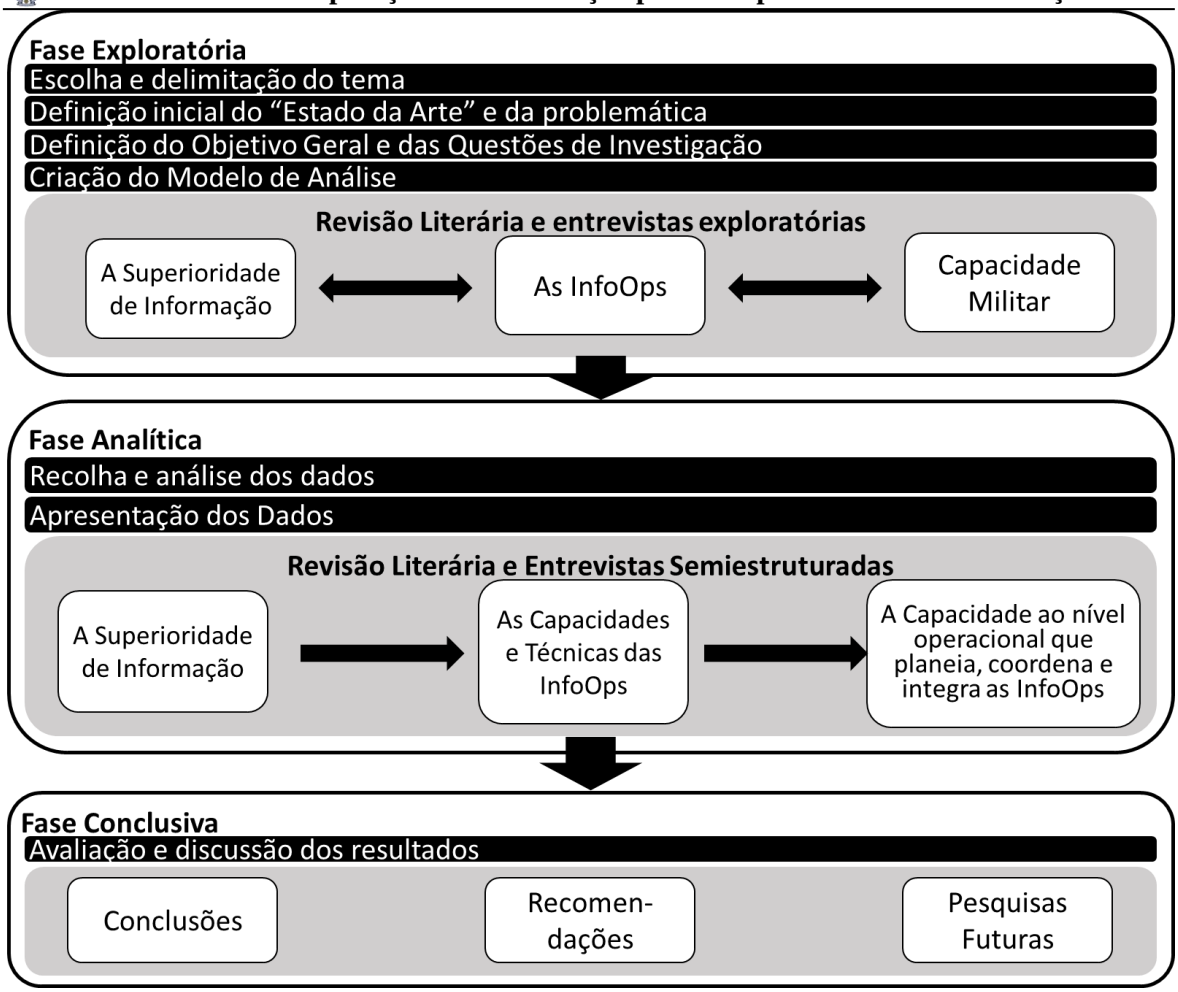



**Figura 4 - Percurso Metodológico**

**Fonte**: Autor (2016c)

# 2. O Caminho para a Superioridade de Informação

Neste capítulo, vamos analisar o conceito de SupInfo, procurando determinar como esta é atingida, que condições são essenciais para a conseguir e como podemos explorar o facto de estarmos numa vantagem de SupInfo. Para tal, será inicialmente descrito o conceito de OCR procurando determinar qual o valor acrescentado de se conduzirem operações em rede. Seguidamente, será descrito o ciclo de tomada de decisão. Por fim, será caracterizada a SupInfo e descritas as condições para a obter e manter.

## 2.1. As Operações Centradas em Rede

> *"… we must achieve: fundamentally joint, network-centric, distributed forces capable of rapid decision superiority and massed effects across the battlespace. Realizing these capabilities will require transforming our people, processes, and military forces."*
> (Rumsfeld, 2003 cit. por. Department of Defense, 2005, p.7)

Vicente (2008, p.53) refere, *"…o conceito GCR*[7] *não é novo, tendo sido adaptado de práticas comerciais. Teve as suas origens na década de 90 na Marinha norte-americana, em resultado de uma nova forma de pensar acerca das operações militares e da vantagem competitiva resultante da superioridade informacional.*". O enfase dado à ligação entre sensores, plataformas de armas e nós do sistema de C2 será maior, em detrimento do enfase no número de plataformas de armas (Potts cit. por Curts e Frizzell, 2005, p.5).

A entidade que melhor define o que entende por OCR é o Departamento de Defesa Norte Americano (DoD). Ribeiro (2008, p.49) resume o entendimento que o DoD faz das OCR como: *"…é entendida como SupInfo, pois facilita a descrição dos conceitos de operações, a organização das forças e a forma como combatem nesta Era da Informação: (i) gera um aumento do poder de combate, devido à interligação em rede de sensores, decisores e sistemas de armas, por forma a obter uma partilha de Consciência Situacional; (ii) um aumento da rapidez de comando e controlo e do ritmo das operações; um aumento da letalidade das armas utilizadas contra o adversário, conjugada com um acréscimo da sobrevivência das forças e um elevado grau de sincronização; (iii) transforma a SupInfo em poder de combate, através da ligação efetiva das forças amigas no Espaço de Batalha, permitindo a partilha da Consciência Situacional*[8] *melhorada e uma ligação rápida aos decisores…*".

Para efeitos deste estudo, modelou-se as OCR de acordo com o proposto por Nunes (2015b). As OCR serão definidas quanto aos domínios chave onde atuam, a sua cadeia de

[7] No artigo original, o autor refere-se à Guerra Centrada em Rede.
[8] Tradução livre do autor

valor a as suas componentes.

2.1.1. Os domínios chave de atuação das OCR

As OCR assentam em 4 domínios chave: (i) O domínio Físico onde o ataque, a defesa e a manobra acontecem utilizando os diferentes ambientes operacionais[9]. Neste domínio todos os elementos da Força estão intimamente ligados em rede e conseguem ter uma conectividade constante e segura; (ii) O domínio da Informação onde a Informação é criada, processada e partilhada. A Força tem a capacidade de recolher, partilhar, ter acesso e proteger a informação. É crucial que a Força seja capaz de colaborar neste domínio; (iii) O domínio Cognitivo onde as perceções, crenças e valores residem e onde, em resultado da compreensão, as decisões são tomadas. A Força tem a capacidade de desenvolver e partilhar uma imagem do ambiente operacional comum e tem um conhecimento partilhado da intenção do comandante; (iv) Por fim o domínio Social onde as diversas entidades da Força interagem. Este domínio implica o impacto cultural que permite criar o entendimento coletivo que, por sua vez, promove a partilha de interações e procedimentos congruentes com a intenção do comandante.

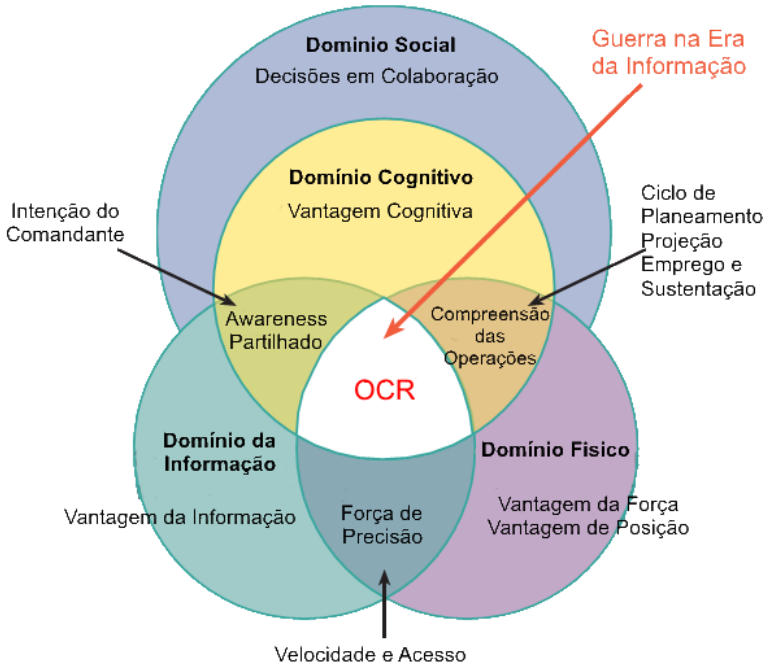



**Figura 5 - Domínios do conflito nas OCR**

**Fonte**: Adaptado de *DoD* (2005, p.21)

A interligação entre os vários domínios pode ser melhor compreendida pelo representado na Figura 5. A partir desta, podemos constatar que os catalisadores de mudança nas capacidades da Força estão onde há uma interceção dos vários domínios. Em última

[9] Terrestre, Marítimo, Aéreo e Espacial.

análise, as OCR ocorrem onde os quatro domínios se intercetam.

#### 2.1.2. Componentes das OCR

As OCR são na sua essência compostas por:

- Redes, que são a fonte da criação de valor;
- Pessoas, que são o fator crítico da mudança;
- Informação, que é o fundamento da decisão.

Estas operações, desenrolam-se no Ambiente de Informação (AInfo). Englobam os fluxos de informação, a capacidade da rede para gerir e explorar essa informação com a finalidade de criar a SupInfo e a superioridade de decisão[10] (Nunes, 2015b).

Havendo redes, que sejam robustas, seguras e de maior cobertura geográfica, leva a que informação relevante e exata seja distribuída no momento certo. Por sua vez, esta partilha, leva à compreensão partilhada da situação, seja ao nível operacional ou estratégico. Uma melhor compreensão da situação, facilita a tomada de melhores decisões, sendo estas mais informadas e geradoras de assimetrias, conferindo à Força uma superioridade de decisão que se converterá numa vantagem operacional. Tomando melhores decisões, planeiam-se e executam-se melhores ações, o que gera maior flexibilidade e agilidade operacional. Assim, obtêm-se efeitos sincronizados, proporcionais e ajustados ao ambiente operacional.

Segundo Ribeiro (2008, p.55), os elementos do espaço de batalha, os componentes das OCR, podem agrupar-se em: Decisores, Sistemas de Armas e Sensores. A Figura 6, abaixo, representa a interligação entre estes elementos.

Ainda segundo este autor (Ribeiro, 2008, p.56), os Decisores, são quem executa o planeamento das operações e exerce o comando e controlo dos Sistemas de Armas e dos Sensores. Os Sistemas de Armas são os executores das ações[11]. São os meios empregues pelas unidades de combate para produzir os efeitos desejados, sejam esses efeitos letais ou não letais. Por seu lado, os Sensores incluem todas as entidades que contribuem para obter a real perceção do Espaço de Batalha. Vão desde as equipas de HUMINT[12], unidades de reconhecimento aos UAV's[13] e satélites, etc.

[10] Apêndice B
[11] Apêndice B
[12] HUMINT: Human Intelligence
[13] UAV: Unmanned Aerial Vehicle (Veículo Aéreo Não Tripulado)

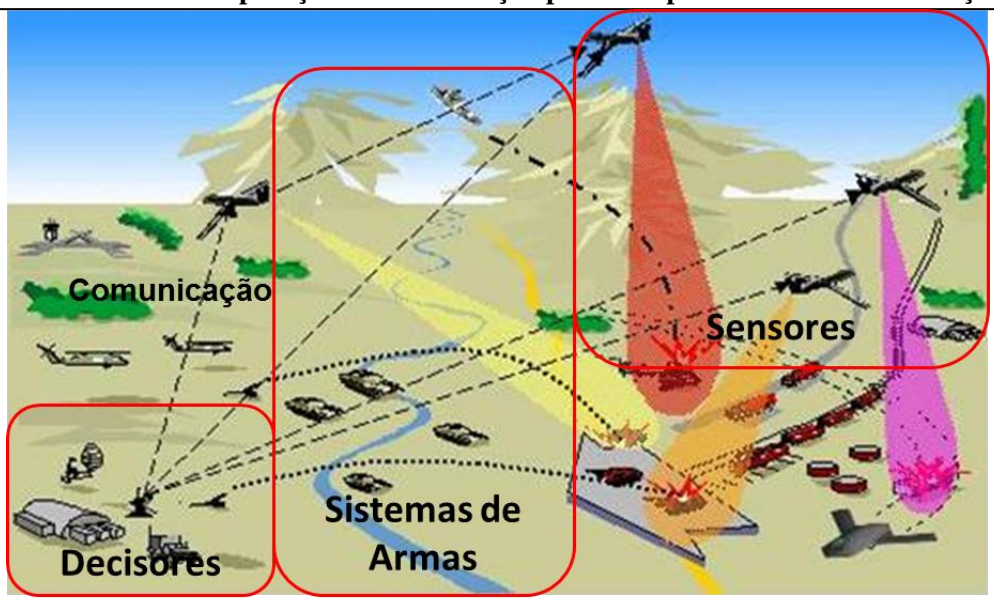



**Figura 6 - Os elementos do Espaço de Batalha**

**Fonte**: Adaptado de Randall (2001, p.3)

Para atingir a SupInfo, estas três componentes devem estar ligadas entre si através de uma rede de sistemas interoperáveis. Só assim se garante que todos os sistemas têm uma visão partilhada do Ambiente Operacional e se obtém a tão almejada colaboração e sincronização das ações.

A interoperabilidade[14] é essencial para garantir que os variados sistemas conseguem estabelecer as ligações que lhes permitem operar na mesma rede. Cada vez mais, as operações militares decorrem num ambiente Conjunto[15] e Combinado[16]. Garantir a troca de informação entre sistemas de várias nações e ramos é essencial para conseguir conduzir as operações de modo condizente com a intensão do comandante da Força. Esta necessidade leva-nos a identificar a arquitetura das OCR.

### 2.1.3. A arquitetura das OCR

Interessa compreender como se relacionam os componentes que permitem a condução das OCR. Stein (cit. por, Ribeiro, 2008, p.57) enumera três componentes funcionais. A rede de Informação, a rede de Combate e a rede de Sensores (Descritas no Apêndice C). A sua relação pode ser observada na Figura 7 abaixo, onde podemos constatar como a integração destas redes, permite a partilha de Informação entre Sensores e Decisores. O resultado materializa-se na produção de efeitos. Como veremos mais à frente, há vantagens em conduzir operações recorrendo ao apoio das redes.

[14] Apêndice B
[15] Conjunto: Operações que englobam o emprego de mais de um Ramo das Forças Armadas (NATO, 2015a, p.2.J.1).
[16] Combinado: Junta Forças de vários países em ambiente de Coligação (NATO, 2015a, p.2.C.8).

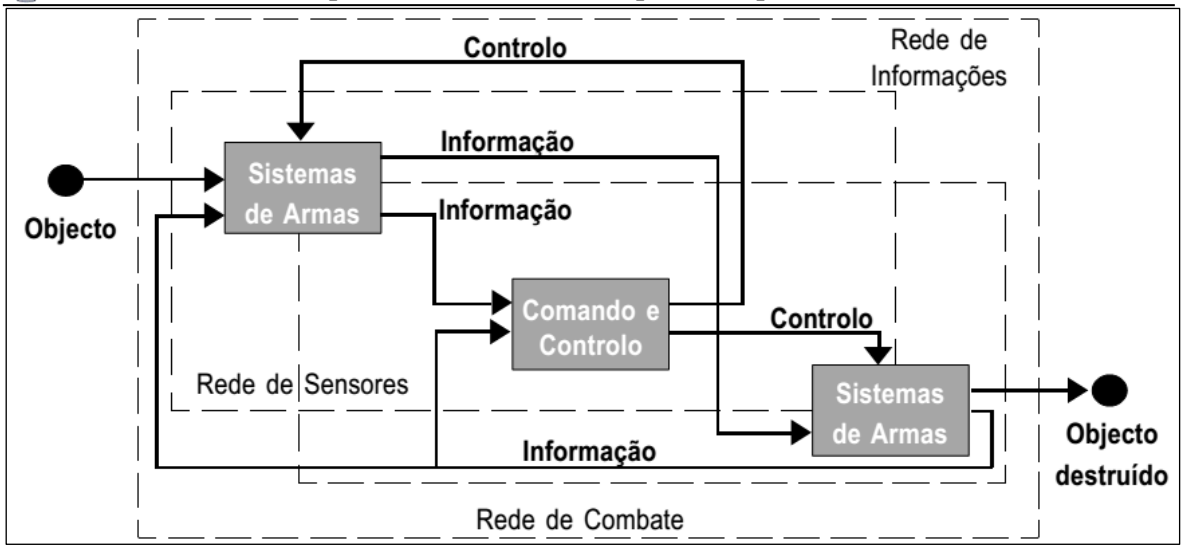



**Figura 7 - A arquitetura das OCR**

**Fonte**: Adaptado de Stein (Ribeiro, 2008, p.57)

### 2.1.4. A Cadeia de Valor das OCR

Para compreender qual a vantagem de se conduzir OCR é preciso compreender quais as hipóteses sobre as quais assenta e os princípios que a orientam. Só deste modo se pode chegar à cadeia de valor e à real vantagem em conduzir OCR. As quatro hipóteses são (Department of Defense, 2005, p.7):

- Uma Força altamente ligada em Rede promove e melhora a partilha de informação;
- A partilha de informação e a colaboração melhoram a qualidade da informação e a consciência situacional partilhada;
- A consciência situacional partilhada leva à auto sincronização da Força;
- Por sua vez, a auto sincronização aumenta drasticamente a eficácia no cumprimento da missão.

Já os princípios que governam as OCR são (Department of Defense, 2005, p.8):

- Lutar pela Superioridade da Informação;
- Acesso à informação: Consciência Situacional Partilhada;
- Rapidez no exercício do comando e na tomada e decisão;
- Auto Sincronização;
- Dispersão de Forças: Operações não contiguas;
- Desmassificação;
- Alcance profundo dos sensores;
- Alterar as condições iniciais a um ritmo de mudança cada vez maior;
- Compressão das Operações e dos níveis da guerra.

A articulação dos princípios com as hipóteses, como pode ser visto graficamente na Figura 8, abaixo, demonstra como se obtém a eficácia no cumprimento da missão, atingindo assim o grande valor acrescentado das OCR. É de igual modo importante observar e ter em conta a relação com os domínios de atuação das OCR. O início do processo ocorre no domínio da informação, sendo neste que se dá a partilha da informação. Esta partilha resulta em alterações ao nível dos processos cognitivos e sociais da Força e das pessoas. Uma alteração nos processos e métodos de trabalho, leva a que no domínio físico, se obtenham efeitos melhores e mais adequados. Em consequência, obtém-se a eficácia no cumprimento da missão.

Em suma, uma Força que opere em rede, permite que o seu comandante desenvolva mais rapidamente uma perceção e compreensão da situação, que comunique informação crítica de forma mais rápida às suas forças e ao escalão superior e reúna as valências necessárias para exercer efeitos em massa contra um adversário.

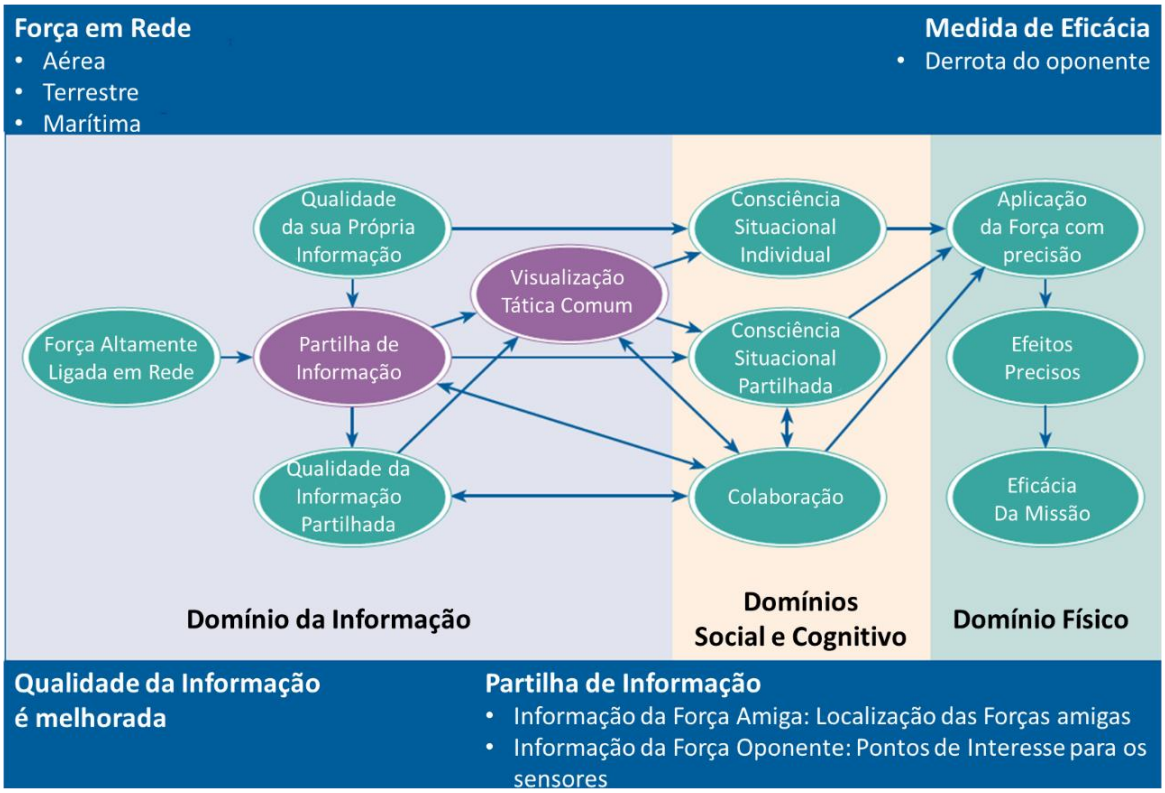



**Figura 8 - A cadeia de valor das OCR**

**Fonte**: Adaptado de DoD (2005, p.23)

## 2.2. O Ciclo de Decisão

Segundo John Boyd, (cit por, Radenović, s.d.), somos rodeados pela ambiguidade e pela incerteza. Boyd argumentava que a nossa incapacidade de dar sentido a uma realidade em constante mudança, é o que nos impede realmente de tomar a decisão correta. "*...quando*

*as nossas circunstâncias se alteram, muitas das vezes, não conseguimos mudar a nossa perspetiva e em vez disso, continuamos a perceber o ambiente que nos rodeia, do modo que pensamos que ele deve ser.*" (Boyd cit. por, Radenović, s.d.).

Fruto da sua experiência em combate enquanto piloto de avião de caça durante a 2ª guerra mundial e guerra da Coreia, Boyd desenvolve o chamado ciclo de OODA[17] (Figura 9). Segundo Boyd, o ciclo representa a sequência de atividades mentais que uma pessoa ou organização desenvolvem aquando a tomada de decisão. Ao alargar o estudo às campanhas militares, conclui que o processo de decisão é semelhante. Nas campanhas analisadas, um dos contendores, conseguiu produzir uma mudança inesperada no Ambiente Operacional, à qual o seu oponente foi incapaz de se ajustar oportunamente.

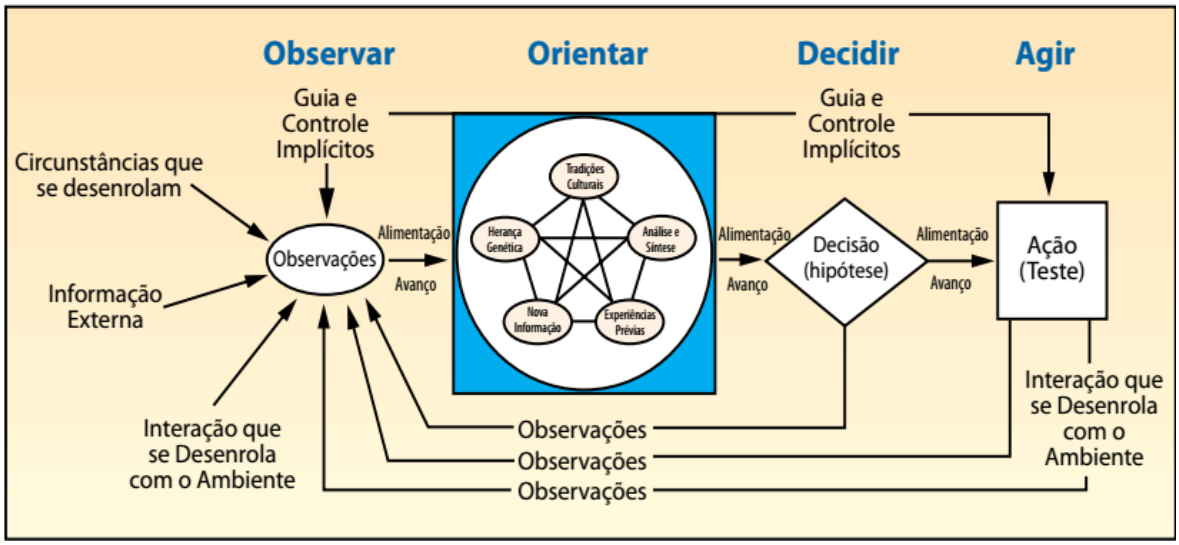



**Figura 9 - O Ciclo de Boyd (OODA)**

**Fonte**: Adaptado de Boyd (Ashley, 2012, p.77)

O ciclo inicia-se com a fase Observar. Aqui o decisor, recebe a informação sobre a situação atual (ambiente envolvente). Recebe informação do exterior, das circunstâncias de momento, de orientações ou ordens que recebe, da interação que tem com o ambiente ou do *feedback* das suas ações. A informação pode chegar até ele proveniente dos seus sentidos, de uma rede de sensores ou de uma rede de Informação. Nesta fase, o decisor, vai processar a informação recolhida durante a fase anterior. Este processamento é afetado pela sua herança genética, pela sua tradição cultural, intuição, formação, pela sua experiência prévia, por nova informação e pela análise e síntese que faz da informação que recebe. Chegado a este ponto, o decisor toma uma decisão efetiva sobre como vai agir. Na última fase, executa a ação e prepara-se para iniciar novo ciclo, recolhendo o *feedback* da sua ação, para o poder alimentar com nova informação.

[17] Observar, Orientar, Decidir, Agir

Analisando o ciclo na ótica da tomada de decisão competitiva, dois oponentes que executem o seu processo de tomada de decisão em paralelo, entram num ciclo vicioso de ação-reação, em que um consegue sempre reagir à ação do outro. Para obter vantagem, um dos oponentes tem de conseguir um *Tempo*[18] operacional superior ao seu adversário, ou em alternativa, criar uma disrupção no processo no seu adversário. Isto pode ser conseguido de duas formas:

- Ou se recorrem a métodos de processamento que fazem uso da tecnologia para a comprimir o ciclo e obter melhores efeitos sobre o adversário (Nunes, 2015c, p.62; Ribeiro, 2008, p.44; Osinga, 2005, p.282);
- Ou criamos uma situação a que o nosso adversário não se consegue adaptar, entrando naquilo a que Boyd designou de entropia mental, o que o leva a não conseguir completar o processo ou, a tomar uma decisão errada (cit. por Radenović, s.d.; Osinga, 2005, p.282).

Isto pode ser conseguido afetando o processamento do seu ciclo de decisão, ou afetando a sua perceção da realidade.

Ao nível Operacional ou Estratégico, Osinga (2005, p.272) refere que devemos estar mais preocupados em operar dentro do espaço temporal da mente do adversário e em gerar diferenças entre os eventos que são observados ou antecipados e aqueles a que deve reagir. Induzindo ações no adversário, conseguimos antecipar os acontecimentos e em consequência, estar preparados para eles. O grande objetivo, é deixar o adversário incapaz de lidar com o desenrolar das circunstâncias.

## 2.3. A Superioridade de Informação

### 2.3.1. Características da Superioridade de Informação

Nunes (2015c, p.63), relativamente ao valor da informação, refere que esta possui um conjunto de atributos únicos e especiais que a diferenciam de qualquer recurso. Já Osinga (2005, p.272) refere que será inútil possuí-la se esta não se traduzir em ação decisiva. Esta afirmação é feita no contexto da análise do ciclo de Boyd e concorre com a opinião de Nunes (2015c, pp.63–64), segundo o qual, a informação por si não possui valor intrínseco. Este valor só é criado quando a informação chega ao seu destinatário. O seu valor é circunstancial e deriva da sua importância relativa para a tomada de decisão ou adoção de uma modalidade de ação. O valor da informação aumenta porque existe a possibilidade de partilha e a realização de uma ação mais eficaz.

[18] Tempo: Considerado aqui como o ritmo a que as Operações se desenrolam

A publicação doutrinária conjunta "JDN 2-13 *Information Superiority*" das FFAA Inglesas (UK MoD, 2013, p.1.4), propõe uma visão adaptativa à SupInfo bem como um conjunto de Características Permanentes[19] e de Princípios[20]. Relativamente à visão adaptativa, é referido que a abordagem à SupInfo e à sua exploração, depende da situação e deve ser orientada para a conduta das operações. Atingir a SupInfo não é um fim em si mesmo, mas um facilitador do cumprimento da missão.

A SupInfo adaptativa permite ao Comandante desenvolver uma compreensão mais correta e intuitiva, bem como desenvolver prospetivas sobre a campanha em curso. Estas, derivam da capacidade de colaborar e dar sentido a situações específicas que têm origem em perspetivas variadas, em especial, é conseguido através da adaptação da visão intuitiva de várias comunidades de interesse. Esta é uma forma em grande parte não técnica, que se tem de atingir a SupInfo ao nível tático e operacional, mas com um possível efeito global. É de igual modo referido que a SupInfo adaptativa, consiste em ganhar uma vantagem competitiva sobre outros atores[21]. Esta vantagem, advém de o Comandante poder dirigir, acionar e empregar os seus recursos no domínio da informação para melhorar o seu processo de tomada de decisão. Advém também, de se poder manipular as perceções dos adversários. A mais valia que se obtém através da influência dos comportamentos dos outros atores, permite uma posição de SupInfo que não deve ser subestimada. As atividades de influência não se devem limitar aos adversários, mas sim a todos os atores. Um exemplo é a influência da opinião das AA através das PSYOPS.

#### 2.3.2. Obter a Superioridade de Informação

Alberts, Garstka e Stein (1999, p.55), referem que o limite do domínio da Informação é alcançado quando a relevância, precisão e temporalidade da informação se aproxima de 100%. Para que tal seja conseguido, podem ser desenvolvidas três tipos de atividades (Alberts, Garstka e Stein, 1999, p.54; Nunes, 2015c, p.66):

- As que servem para melhorar o processo de reunião, processamento e disseminação da informação necessária (no caso das Forças militares o C4ISR).
- As que permitem proteger estas atividades e garantir o fluxo e integridade da informação (capacidade de condução de InfoOps[22] defensivas e Garantia de Informação[23]).

[19] Tabela 2 - Anexo A
[20] Tabela 3 - Anexo A
[21] Apêndice B
[22] O conceito de InfoOps será abordado no próximo capítulo.
[23] Information Assurance (Apêndice B)

– As que permitem degradar/reduzir a posição do adversário no domínio da informação (InfoOps ofensivas).

Os efeitos que se pretendem obter podem ser vistos nas Figura 10 e Figura 11. Aplicando as medidas que servem para melhorar o processo de reunião, processamento e disseminação de informação, bem como as que permitem proteger a nossas atividades e garantir o fluxo e integridade de informação, iremos potenciar e aumentar a nossa posição no domínio da informação. Já para reduzir a posição do adversário, iremos aplicar medidas para degradar ou reduzir a sua capacidade de reunir, processar e disseminar informação.

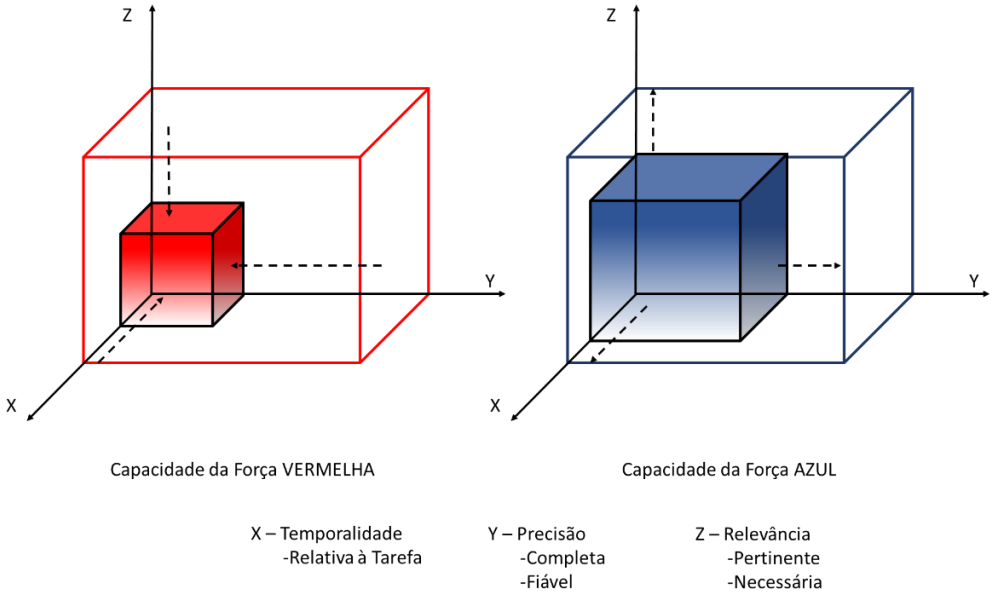



**Figura 10 – Efeitos sobre a posição no domínio da Informação**

**Fonte**: Adaptado de Alberts, Garstka e Stein (1999, p.56)

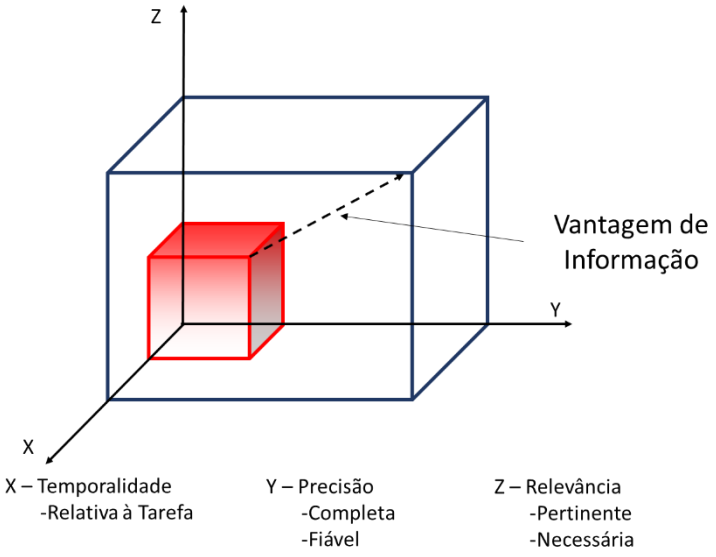



**Figura 11 - Posição de Superioridade de Informação**

**Fonte**: Adaptado de Nunes (2015c, p.64)

### 2.3.3. Condições para se obter a Superioridade de Informação

A publicação doutrinária das FFAA Inglesas JND 2-13 (UK MoD, 2013, p.2.1), refere que o Comandante, deve procurar atingir uma posição de superioridade no domínio da Informação, quer em campanha, quer nas atividades do dia-a-dia. Quando em operações, deve procurar compreender a ameaça, melhorar a proteção, a resiliência e integrar as perspetivas de todos os que podem tomar decisões. Para tal, o comandante deve promover um conjunto de atividades que visam manter o seu EM preparado para atingir as condições para obter a SupInfo. Essas atividades devem ser conduzidas quando a Força conduz o seu treino regular, durante o treino de aprontamento para uma missão específica, durante a recuperação de uma missão e quando está aquartelada. Mais especificamente, essas ações são:

- Durante o aprontamento: Devem ser identificadas:
  - As vantagens que se devem procurar atingir no domínio da Informação;
  - A Compreensão que se tem da Situação;
  - Os *Enablers* a implementar e a ativar (avaliar a necessidade de planos de contingência e de medidas de mitigação para as situações em que se não se atinge o estado de SupInfo);
  - Os processos que garantem que os *Enablers* permitem a necessária flexibilidade e agilidade.
- Durante a missão: Implementar Medidas de Eficácia (MoE) para monitorizar o grau e a natureza da SupInfo detida pela Força;
- Durante o período de regeneração: Devem estar implementados processos que permitam a captura de Observações para alimentar o processo de Lições Aprendidas;
- Quando aquartelada, a Força deve manter os mesmos procedimentos e mentalidade no que respeita à gestão e processamento de Informação. A possibilidade de ciberataques é permanente, pelo que se devem manter as atividades de proteção da Informação. Deve-se de igual modo, manter uma avaliação constante, dos possíveis cenários de emprego da Força.

Podemos enunciar como condições para se atingir a SupInfo (UK MoD, 2013, p.2.5; US ARMY, 2001, p.11.20; Alberts, Garstka e Stein, 1999, p.54):

- Uma rede de sistemas interoperáveis[24];

[24] Parágrafo 2.1.2

- Pessoal competente e treinado que seja capaz de colaborar, partilhar e utilizar a informação corretamente, e ajustar o comportamento dos sistemas e os níveis de interoperabilidade;
- Níveis adequados de gestão de informação e do conhecimento (GIC);
- Serviços de tecnologias de informação (TI) que permitam obter uma Visão Operacional Partilhada e ferramentas rápidas, intuitivas e que permitam manter um fluxo ininterrupto de Informação (*e.g*. capacidade de indexação e pesquisa de informação);
- Planeamento e preparação;
- Integração vertical e horizontal de capacidades como o IVR[25];
- Procedimentos adequados de Garantia de Informação e de proteção das redes;
- Capacidade de explorar ou negar ao adversário a utilização do AInfo.

Nunes (2017) concordando com a totalidade das condições acima indicadas, refere que estas se encontram na sua maioria nos domínios Físico e Informacional, sendo necessário evoluir para condições no domínio Cognitivo. É preciso estabelecer uma consciência partilhada da situação. Esta é conseguida, criando processos comuns e através da fusão da informação. Só assim se atingirá uma visão comum que vai produzir decisões alinhadas.

Assim, para aplicar estas medidas e garantir as condições para se obter a SupInfo, é necessário que os envolvidos, usem o seu intelecto, vontade, capacidade de avaliação e engenho. Para executar a avaliação do AInfo, os EM devem conduzir em permanência o Estudo do AInfo (NATO, 2015b, p.A-1-A-5; UK MoD, 2013, pp.2-2-2–5).

#### 2.3.4. Explorar a Superioridade de Informação

Após se ter atingido um estado de SupInfo, é necessário mantê-lo. É difícil a qualquer um dos oponentes manter uma posição de vantagem no domínio da Informação (Figura 12), pelo que a condução de operações neste domínio deve ser constante. Ambos os oponentes, procurarão conduzir as ações anteriormente referidas para proteger as suas capacidades e para degradar as do adversário.

[25] Informações, Vigilância e Reconhecimento

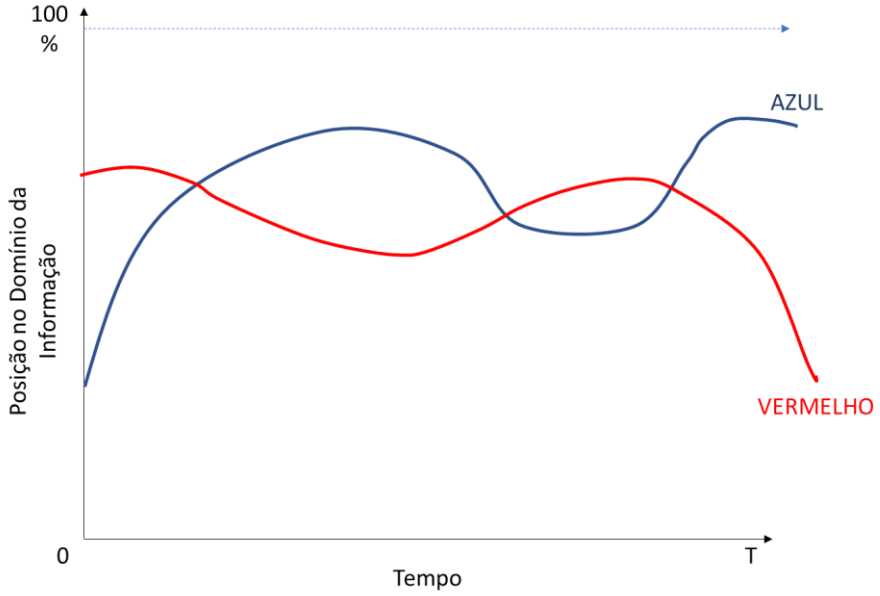



**Figura 12 - Variação da Posição dos oponentes no domínio da Informação**

**Fonte**: Autor (2017)

Este estado de vantagem, constitui-se como um multiplicador de potencial de combate. A Figura 13, abaixo, exemplifica a relação das atividades que se devem desenvolver para atingir a SupInfo e o Ciclo de Boyd. Cada um dos oponentes desenvolve as referidas atividades para proteger o seu processo de decisão e a sua posição no domínio da informação, enquanto procura degradar ou reduzir a posição do seu adversário.

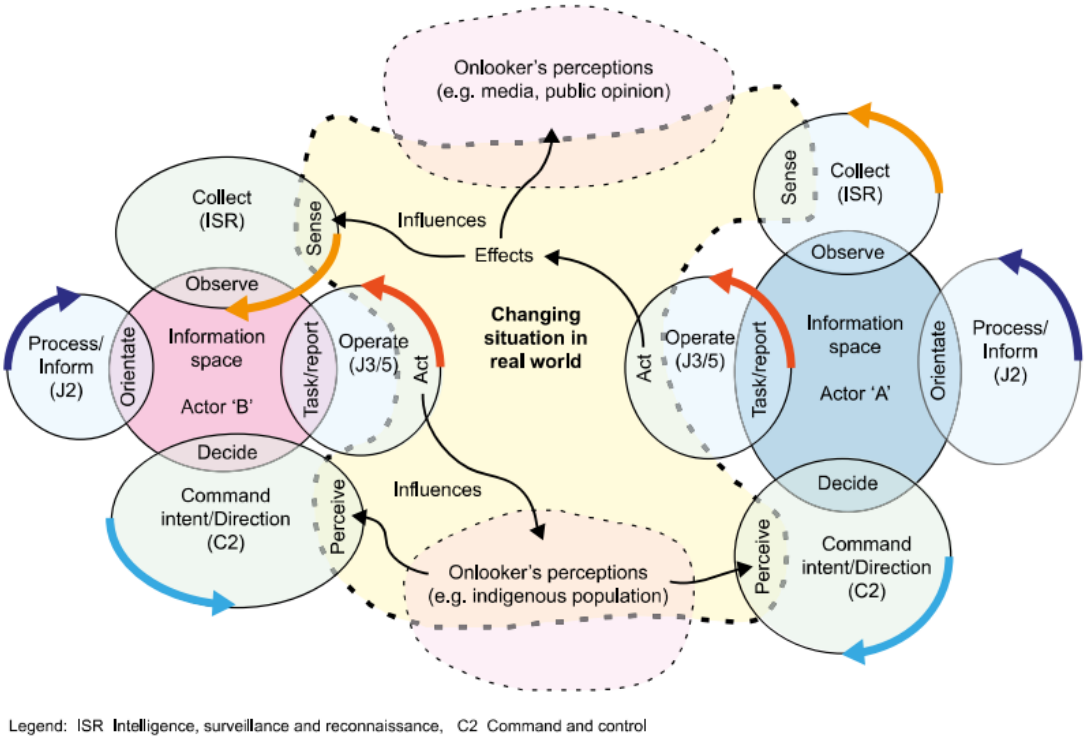



**Figura 13 - Interação entre dois oponentes que procuram obter superioridade de informação**

**Fonte**: UK MoD (2013, p.3.5)

O ciclo *Collect* é acionado pela necessidade de se perceberem as alterações ao ambiente, inclusive as que são provocadas pelas próprias ações. As observações subsequentes, alteram o AInfo. O ciclo *Process* acrescenta valor e significado ao AInfo, alimentando o processo de tomada de decisão e resolução de problemas dos ciclos subsequentes. O ciclo *Command* é onde a intenção, a orientação e direção do comandante são desenvolvidas através de discernimento e previsão informados pelas perceções que o Comandante tem do AInfo. No ciclo *Operate*, são produzidos os efeitos (físicos e de influência) sobre os adversários. Usa o AInfo para atribuição de tarefas e de processamento de relatórios (UK MoD, 2013, p.3.6).

# 3. Caracterização das Operações de Informação

Neste capítulo, serão descritas as InfoOps procurando determinar qual o seu produto operacional. Para tal, inicialmente será caracterizado o AInfo. Seguidamente serão enunciados os fundamentos das InfoOps, onde serão abordadas as áreas relacionadas das InfoOps, a finalidade de conduzir InfoOps e serão descritas as capacidades e técnicas das InfoOps. Por fim, será analisado o produto combinado de cada uma das capacidades e técnicas das InfoOps.

A incorporação das InfoOps na doutrina da NATO, decorre da aplicação do conceito de Guerra de C2 durante a 1ª guerra do Golfo (1990/91). Na altura, o plano de campanha das Forças aliadas, lideradas pelo Gen. Norman Schwartzopf, incluía isolar a estrutura de C2 das Forças Iraquianas das suas unidades no terreno. Na sequência desta campanha, em 1995, a NATO desenvolve o conceito de *Command and Control Warfare* (C2W). No entanto, a própria NATO refere que as InfoOps não são a continuação, nem substituem a C2W. Pelo contrário, há atividades de informação (AI) que contribuem para a C2W. As InfoOps estão orientadas para o aconselhamento e coordenação de efeitos no AInfo no seu sentido mais lato. Estes efeitos podem resultar de atividades conduzidas no âmbito da C2W (NATO, 2010, pp.10–11).

## 3.1. O Ambiente da Informação

Para a NATO (2015b, p.1.2-1.3) as InfoOps desenrolam-se no designado, AInfo. Este é composto por duas características principais, os domínios e as relações entre estes (Figura 14).

No que diz respeito aos domínios temos:

- O domínio Cognitivo, onde se tomam as decisões;
- O domínio Virtual, onde ocorre uma atividade intangível e onde as ferramentas técnicas facilitam a comunicação (anteriormente descrito como domínio de Informação, Parágrafo 2.1.1);
- O domínio Físico, o espaço onde as atividades físicas ocorrem e os indivíduos, nações, estados, culturas e sociedades interagem.

Já as relações entre os domínios, ocorrem entre as seis camadas do AInfo. As camadas são (NATO, 2015b, p.1.3):

- O mundo real e os seus eventos;
- A conetividade da rede que suporta a transferência de informação;
- A Informação;

- As pessoas que desenvolvem as mensagens e os conteúdos que circulam no AInfo;
- A quinta e sexta camadas são compostas pelas pessoas (singulares e grupos sociais) que interpretam e exploram o AInfo.

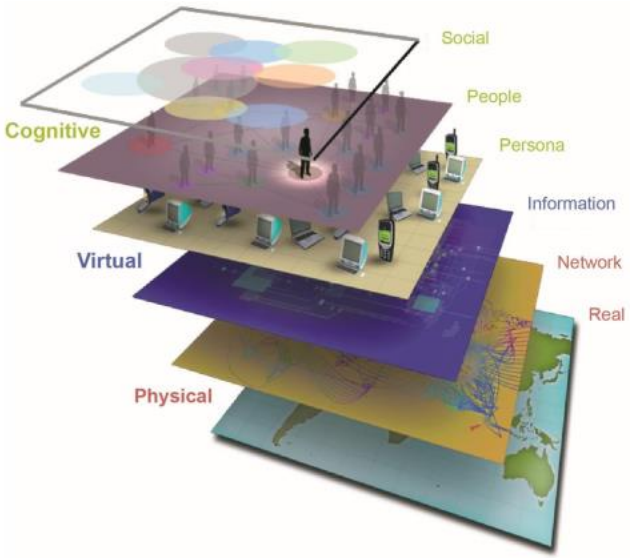



**Figura 14 - O Ambiente de Informação**

**Fonte**: NATO (2015b, p.1.2)

Podemos traçar um paralelo entre o AInfo e os domínios chave onde se desenrolam as OCR (Parágrafo 2.1.1). De facto, representam o mesmo ambiente. Não obstante da representação por camadas da Figura 14, a ideia de domínios que se intercetam (Figura 5) é uma representação mais aproximada do que se passa na realidade.

### 3.2. Operações Baseadas em Efeitos

Smith (2003 cit. por Nunes, 2015c, p.193) diz-nos que a probabilidade sucesso de um ator num conflito ou crise, varia de acordo com a relação entre os meios disponíveis e a sua vontade de expressa para o vencer. Smith propõe mesmo que a probabilidade de sucesso varia aritmeticamente com os meios ao dispor, e geometricamente com a vontade de o travar. Assim, um ator com meios mais limitados, pode fazer face a um outro com mais meios, desde que a sua vontade para travar o conflito seja maior. Do mesmo modo, podemos daqui concluir que, afetando a vontade do ator adversário, podemos levá-lo à capitulação. O estudo da conflitualidade ao longo da história, tem exemplos de como se atingiram objetivos (*Ends*), através da acumulação de efeitos no domínio físico (destruição dos seus meios) e no domínio cognitivo (afetação da sua vontade). A retirada de Massena perante as linhas de Torres em 1811, é disso um exemplo.

A NATO (2010, cit. por Moller, 2014, p.179) define Operações Baseadas em Efeitos[26] (OBE) como "*…a aplicação coordenada e compreensiva dos vários instrumentos de poder da Aliança, combinada com a cooperação prática com outros atores envolvidos na operação de modo a criar os efeitos desejados e consequentemente atingir o estado final desejado pela Aliança*.". Por seu lado, Vicente (2006, pp.238–239) refere que a produção de efeitos que se procura com a condução de OBE, sofre um salto qualitativo quando combinada com as OCR. Podemos então inferir que é fruto desta combinação, que se materializa o valor acrescentado de conduzir OCR.

O conceito de OBE está intimamente ligado à análise sistémica das capacidades do adversário. Em vez de procurar exclusivamente a destruição física do adversário, as OBE, tentam orientar-se para a produção de efeitos coordenados e encadeados, num sistema, afetando os seus nós críticos através do reforço ou eliminação da sua capacidade de ligação e interação (Nunes, 2015c, p.199).

Procura-se antes de mais, condicionar os comportamentos do adversário. De notar, como foi referido anteriormente, que não se deixam de produzir efeitos físicos, estes são é complementados com a busca da disrupção dos seus processos de tomada de decisão, procurando assim afetar os seus comportamentos. É ainda importante referir que os efeitos podem ser diretos (de 1ª ordem), que são na sua essência físicos (mas podem ser atingidos nos domínios Físico e da Informação), ou secundários (de 2ª ordem), que são os que se fazem sentir nas perceções e/ou ao nível psicológico e afetam a vontade do adversário (Vicente, 2006, pp.237–238; Nunes, 2015c, p.196). Este processo, pode ser visto de forma gráfica na Figura 15.

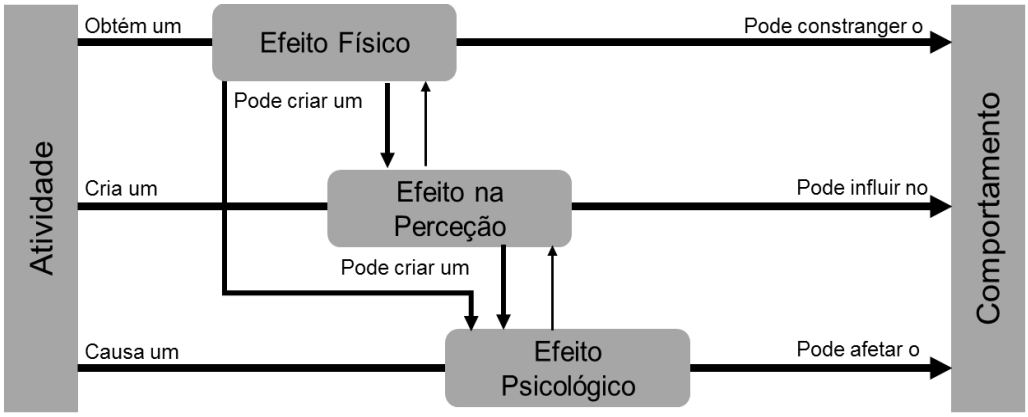



**Figura 15 - Sequência da geração de efeitos**

**Fonte**: Adaptado de MNOE (2004, cit. por Nunes, 2015c, p.196)

Smith (2003, pp 430-435 cit.por Nunes, 2015c, p.199) sistematiza um conjunto de

[26] Na NATO, designadas por *Effects Based Approach to Operations* (EBAO)

princípios básicos para as OBE:

- As ações geram efeitos diretos e indiretos;
- Os efeitos têm uma dimensão física e psicológica;
- Os efeitos ocorrem simultaneamente aos níveis estratégico, operacional e tático, refletindo-se em múltiplas áreas;
- Os efeitos estão interrelacionados e são cumulativos.

### 3.3. A Guerra de Informação

Stein, (1995, cit. por Schechtman, 1996, p.29) refere que *"A Guerra de Informação, é na sua essência influenciar outros seres humanos e o seu processo de decisão. Pode assim afirmar-se que o alvo da Guerra de Informação é a mente humana, especialmente aquelas mentes que tomam as decisões chave sobre a paz e a guerra. De uma perspetiva militar, aquelas mentes que tomam as decisões chave sobre Se, Quando, e Como serão empregues os meios e capacidades das suas estruturas estratégicas (militares)."*

Já Dinis (2005, pp.65–67), associa o conceito de GI ao de InfoOps, enquadrando-a no espectro da conflitualidade. Refere que a GI tem como elemento base a Informação e que esta apresenta aspetos complementares que visam explorar a informação disponível, proteger a nossa informação e ganhar a batalha das perceções.

Nunes (2015c, pp.179–180), enquadra a GI ao nível Estratégico, referindo a dualidade do conceito, que tanto tem aplicações militares como civis. Para este estudo, apenas nos interessa considerar as aplicações militares da GI. No entendimento deste autor, a GI na sua vertente militar é conduzida ao nível Político-Estratégico. É assim possível otimizar os seus efeitos e atingir os objetivos nacionais ou organizacionais. Ao fazer a ponte para o nível Operacional, considera as InfoOps como a continuação da GI. Por sua vez, ao nível tático é conduzida a Guerra de Comando e Controlo (C2W), que é entendida como sendo *"... o conjunto de atividades desenvolvidas com o objetivo de proteger o nosso ciclo de tomada de decisão enquanto simultaneamente se ataca o processo de decisão do adversário. Constituindo por excelência uma "guerra de decisão", procura criar as condições necessárias a uma decisão mais rápida do e eficaz tendo em vista a obtenção do sucesso operacional."* (Nunes, 2015c, p.180).

### 3.4. Fundamentos das Operações de Informação

Tendo o conceito de InfoOps sido definido no parágrafo 1.2.5 (pode ser observado graficamente na Figura 16) juntamente com as áreas interrelacionadas, importa definir o que

se entende por AI, "*Ações destinadas a afetar a informação ou os sistemas de informação*[27]. *As AI podem ser desenvolvidas por qualquer dos atores e incluem medidas de proteção*" (NATO, 2015b, p.1.5). Estas podem ser letais e não letais, devendo ser integradas entre si, orientadas pelo planeamento e avaliadas durante a execução da operação. Procura-se assim, produzir efeitos psicológicos e físicos em todos os domínios do AInfo (NATO, 2015b, pp.1.4-1.5).

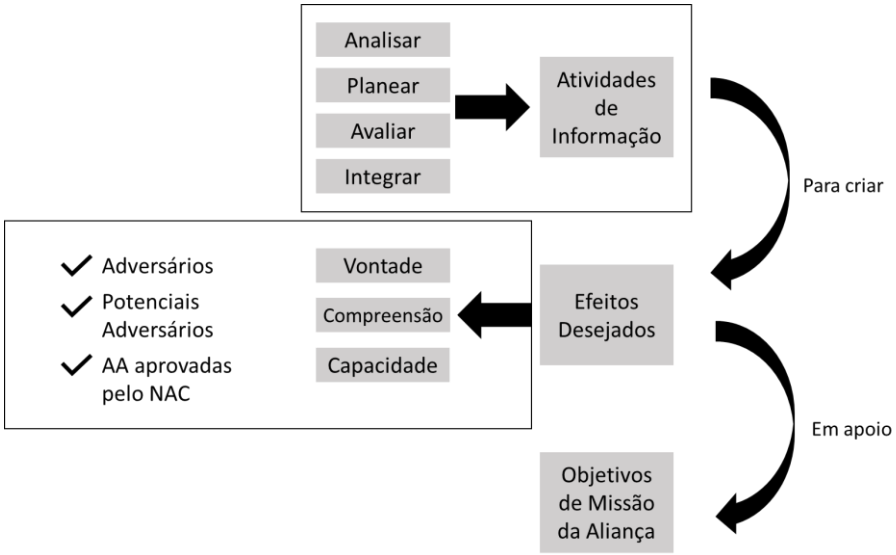



**Figura 16 - As InfoOps**

**Fonte**: Adaptado de NATO (2015b, p.1.6)

Sendo uma função de EM, as InfoOps são mais orientadas para o AInfo, não sendo uma capacidade em si. Providenciam ao Comandante uma avaliação do AInfo e os mecanismos para executar o planeamento e a coordenação continua das AI, de modo a produzir os efeitos desejados em apoio aos objetivos operacionais. Integram o emprego de um conjunto de capacidades, ferramentas e técnicas para conduzir AI, bem como para proteger o processo de tomada de decisão da influência de atores externos (NATO, 2012, pp.2–3).

Para a NATO (2012, p.4) as InfoOps são conduzidas ao nível Estratégico, Operacional e Tático, sendo neste último que os efeitos pretendidos são produzidos. No entanto, de modo a garantir a sincronização de efeitos e o alinhamento de decisão anteriormente referidos, as InfoOps devem ser planeadas numa perspetiva de *Top-Down*, ou seja, do nível Operacional para o Tático. O enquadramento e alinhamento com os níveis das operações[28] que a NATO faz das InfoOps, pode ser observado na Figura 17.

Daqui decorre a importância de haver, ao nível Operacional, a capacidade militar de

[27] Apêndice B
[28] Descritos no Parágrafo 4.1

executar a análise do AInfo[29], conduzir o planeamento, avaliação e integração das diversas AI.

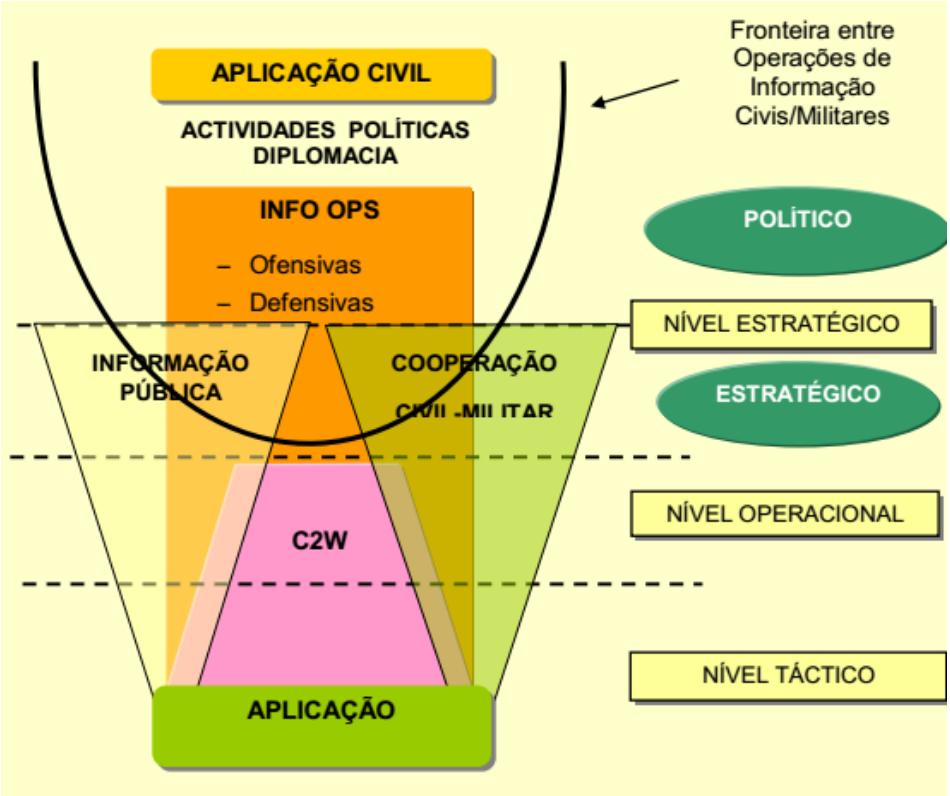



**Figura 17 - Modelo de Enquadramento das InfoOps na NATO**

**Fonte**: Adaptado de Segura (EME, 2011, p.51)

### 3.4.1. As Áreas Interrelacionadas das InfoOps

Doutrinariamente a NATO (2015b, p.1.6, 2012, p.4) desenvolve AI segundo três áreas interrelacionadas e que visam:

- Preservar e Proteger continuamente a liberdade de ação da Aliança no AInfo. É conseguido defendendo os dados, a informação e as redes que apoiam os processos de decisão e os decisores da Aliança[30], e podem ser designadas de InfoOps defensivas.
- Os comportamentos, perceções e atitudes das AA aprovadas pelo NAC, com a finalidade de induzir, reforçar, convencer ou encorajá-las a apoiar os objetivos da Aliança[31].
- Contrariar a propaganda adversária e as suas funcionalidades e capacidades de C2 que apoiem a sua formulação de opinião e o seu processo de tomada de

[29] Como referido no parágrafo 2.3.3, esta análise é conduzida elaborando o Estudo do AInfo.
[30] Doravante designadas por "Proteção de Informação"
[31] Doravante designadas por "Atividades de Influência"

decisão[32], e que em conjunto com a área anterior são consideradas InfoOps Ofensivas.

### 3.4.2. A Finalidade das InfoOps

A NATO (2015b, p.1.7-1.9) entende que a eficácia de um ator[33] é uma função da sua Vontade de agir, da Compreensão que este faz da situação e do AInfo e por fim, da sua Capacidade de agir, recorrendo aos meios de que dispõe. Se qualquer um destes três elementos estiver em falta, as decisões e ações do ator serão afetadas. As atividades coordenadas através das InfoOps, visam afetar qualquer um destes elementos.

A Vontade é a capacidade do ator em decidir iniciar uma modalidade de ação. Inclui a sua motivação para agir, as suas atitudes, crenças e valores, bem como a intenção de agir ou resistir. As AI reforçam ou dissuadem determinados comportamentos nas AA aprovadas. Do mesmo modo, deverão ser conduzidas AI para preservar a Vontade dos atores da Aliança em prosseguir os seus objetivos.

A Compreensão, por seu lado, dá contexto, perspetiva e prospetiva, às perceções e à interpretação de uma situação. Este contexto, permite a tomada de decisão com a consciência dos resultados. As AI visam negar, degradar, desarticular ou apresentar informação às AA de modo a afetar as suas perceções e Compreensão. No caso da Aliança, visam assegurar a disponibilidade de informação para os decisores. Assim é possível garantir a Compreensão partilhada entre os membros da Aliança e parceiros, o que melhora o processo de tomada de decisão e a eficácia.

A Capacidade são os meios que o ator dispõe para agir. As AI procurarão afetar esses meios (Ex. C2, Infraestrutura de Comunicações, Instalações de difusão de propaganda) que permitem aos atores a Compreensão da situação e a aplicação da sua vontade de agir. Assim, as AI procuram degradar, destruir, enganar, desarticular e negar as capacidades que permitem aos decisores adversários aumentarem o seu Compreensão do AInfo e impor ou aplicar a sua Vontade e quando apropriado, exercer o C2 das suas Forças. As AI também serão empregues para atacar a fonte de poder (Centro de Gravidade)[34] ou de legitimidade de um adversário. O objetivo é influenciar o seu processo de tomada de decisão, impedindo que tome a iniciativa. Do mesmo modo, as AI serão empregues para proteger as capacidades de C2 e Comunicações e Sistemas de Informação das Forças amigas de modo a permitir que se exerça o C2 e ganhar e manter a iniciativa.

[32] Doravante designadas por "Atividades Anti-C2"
[33] Apêndice B
[34] Apêndice B

#### 3.4.3. Capacidades e Técnicas das InfoOps

Seguidamente, far-se-á uma breve descrição de cada uma das capacidades e técnicas integradas pelas InfoOps e como contribuem para atingir os objetivos da campanha.

##### 3.4.3.1. Operações Psicológicas

O principal objetivo das PSYOPS é influenciar os comportamentos, perceções e atitudes das AA aprovadas pelo NAC. Fornecem a principal capacidade de analisar e contrariar a propaganda realizada pelo adversário. As PSYOPS mantêm o controle direto sobre o conteúdo e a disseminação inicial das suas atividades e mensagens (NATO, 2015b, p.1.10).

##### 3.4.3.2. Guerra Eletrónica

A utilização do espetro eletromagnético é comum a todos os atores, pelo que a livre utilização deste espetro é vital para a condução de operações. A GE desenvolve atividades que permitem proteger e negar a utilização do espetro eletromagnético. Estas atividades são: Contra Medidas Eletrónicas (CME) de ataque, Medidas de Proteção Eletrónica (MPE) de proteção e Medidas de Apoio Eletrónico (MAE) de exploração. Os efeitos da GE podem ser permanentes ou temporários e são não-letais, pelo que possibilitam que se evitem danos colaterais (NATO, 2015b, p.1.11; Rego, 2016, p.26).

##### 3.4.3.3. Operações no Ciberespaço

As CyberOps[35] visam utilizar capacidades para criar efeitos através do ciberespaço em apoio dos objetivos definidos. Podem ser Ofensivas e Defensivas e dividem-se em (NATO, 2015b, p.1.12; Rego, 2016, pp.30–31; US Dod cit. por IDN, 2013, p.12):

- Computer Network Attack (CNA): ações desenvolvidas através da utilização de redes de computadores para interromper, negar, degradar ou destruir a informação tratada pelas redes de comunicações e pelos sistemas de informação (do adversário).
- Computer Network Exploitation (CNE): Capacidades de recolha de informações levadas a cabo através do uso de redes de computadores para recolher dados das redes de comunicações e dos sistemas de informação de um potencial adversário.
- Computer Network Defence (CND): Medidas adotadas através da utilização de redes de computadores para proteger, controlar, analisar, detetar e responder a atividades não autorizadas nos sistemas de informação e comunicações. As

[35] A NATO está a rever o conceito de CyberOps. Estas passarão a dividir-se em Ofensivas e Defensivas (Rego, 2017). No entanto, a publicação doutrinária que revê e atualiza o conceito, ainda não está aprovada, pelo que se convencionou manter a designação atual.

ações CND não procuram apenas proteger os sistemas amigos de um adversário externo, mas também contemplam a possibilidade de a sua exploração ocorrer a partir do interior da própria organização.

#### 3.4.3.4. Presença, Postura e Perfil

Só por si, a presença da Força pode ter um efeito nas perceções. A PPP de uma Força e da sua liderança transmitem uma mensagem aos restantes atores. Os elementos do EM com responsabilidade nas InfoOps, devem aconselhar o modo como a PPP pode ser conduzida para ter impacto no AInfo (NATO, 2015b, p.1.12-1.13).

- Presença: A presença ou a ameaça de destacar uma Força, tem impacto nas perceções, reforçando a credibilidade da mensagem que se pretende transmitir.
- Postura: A postura e conduta da Força na Área de Operações (AO) pode ser escrutinada pela opinião publica, devendo ser tidos em conta fatores como as diferenças culturais e a ameaça.
- Perfil: O perfil público do Comandante também será ele sujeito ao escrutínio tendo um impacto nas perceções dos outros atores.

#### 3.4.3.5. Deceção

A Deceção compreende as medidas que visam enganar o adversário através de manipulação, distorção ou falsificação de provas, a fim de levá-lo a agir de um modo contrário aos seus interesses. Envolve medidas que manipulem as perceções e condicionem os comportamentos dos decisores adversários de modo a serem persuadidos a adotar uma modalidade de ação. A Deceção visa influenciar o seu processo cognitivo, criando efeitos físicos nas suas atividades (NATO, 2015b, p.1.13).

#### 3.4.3.6. Segurança das Operações (OPSEC)

A OPSEC emprega medidas passivas e ativas, que visam negar ao adversário conhecimento sobre o dispositivo, capacidades e intenções das Forças amigas. Identifica e protege Informação que é vital para o sucesso da operação. Esta Informação é designada por Elementos Essenciais de Informação Amiga. Negando esta Informação aos decisores adversários, está-se a afetar a sua Compreensão do Ambiente Operacional (NATO, 2015b, p.1.14).

#### 3.4.3.7. *Engagement*[36]

O *Engagement* é o termo usado para descrever a atividade de relacionamento direto

[36] Não havendo termo em português que exprima convenientemente o conceito, o autor decidiu usar o termo em Inglês.

entre as lideranças e entre os elementos da Força e a população em geral. Este relacionamento dever ser permanente e a todos os níveis. Só assim produz efeitos ao nível dos comportamentos, atitudes e perceções das AA. Estas atividades de relacionamento, devem ser consistentes, sensíveis às diferenças culturais, credíveis, balanceadas e pragmáticas. A interação entre lideranças e pessoas de interesse, designa-se por KLE[37], já entre a Força e a população designa-se por *Soldier Engagement*.

O KLE pode ser usado para influenciar a Liderança de uma AA a apoiar os objetivos da Aliança. Já as atividades de *Soldier Engagement* devem ser conduzidas continuamente e estão diretamente relacionadas com as atividades de PPP. Podem ser deliberadas, quando são programadas e têm um objetivo especifico, ou dinâmicas quando ocorrem espontaneamente e fruto de um aproveitamento das circunstâncias.

#### 3.4.3.8. Destruição Física

A Destruição Física contribui para as InfoOps de duas maneiras. Primeiro, destruir fisicamente sistemas de C2 afeta a Capacidade, a Vontade e a Compreensão do adversário. Segundo, a aplicação da Força produz um impacto psicológico no adversário. O emprego da Força, quando devidamente dirigido e mesmo que limitado, tem efeitos dissuasores no adversário, pode coagi-lo e reduz a sua capacidade de exercer o comando das suas Forças. Deve-se pesar o risco de provocar danos colaterais, com um efeito negativo nas perceções das AA com os benefícios esperados dos efeitos que se pretendem obter (NATO, 2015b, p.1.16).

#### 3.4.3.9. Cooperação Civil Militar

A CIMIC promove e facilita a coordenação e cooperação (em apoio da nossa Missão) com os atores civis, incluindo a população, autoridades locais, Organizações Internacionais e Organizações Não Governamentais. A Força deve planear e desenvolver as ações CIMIC sem que estas sejam percecionadas como atividade de recolha de informações. A CIMIC não é uma AI, no entanto as suas ações devem ser integradas com as InfoOps, uma vez que enviam mensagens diretas e indiretas às AA. Como tal, contribui para obter efeitos no AInfo. A CIMIC permite afetar a Vontade e a Compreensão do adversário (NATO, 2015b, p.1.11-1.12, 2012, pp.6–7).

#### 3.4.3.10. Informação Pública

Não sendo uma Capacidade ou Técnica coordenada pelas InfoOps, as PA devem ser integradas de modo a garantir a consistência da mensagem com as atividades de PSYOPS.

[37] *Key Leader Engagement*

Assim, assegura-se a credibilidade da Força e a coordenação de esforços para a persecução dos objetivos da Aliança. A PA permite contrariar a desinformação do adversário e dissuadir a sua ação (NATO, 2015b, p.1.16, 2012, p.6).

#### 3.4.4. O Produto Combinado das InfoOps

O produto das Capacidades e Técnicas das InfoOps para as AI e para a sua finalidade, pode ser resumido segundo a Tabela 1, abaixo.

**Tabela 1 - Produto das Capacidades e Técnicas das InfoOps**

| | Áreas de Atividade | | | Finalidade | | |
|---|---|---|---|---|---|---|
| | InfoOps Defensivas | InfoOps Ofensivas | | Vontade | Compreensão | Capacidades |
| | Proteção Informação | Influência | Anti-C2 | | | |
| PSYOPS | | ■ | ■ | ■ | ■ | |
| GE | ■ | | ■ | ■ | ■ | ■ |
| CyberOps | ■ | | ■ | ■ | ■ | ■ |
| PPP | | ■ | | | ■ | |
| Deceção | | ■ | | | ■ | |
| OPSEC | ■ | | | | ■ | |
| *Engagement* | | ■ | | ■ | ■ | |
| Destruição Física | | ■ | ■ | ■ | ■ | ■ |
| CIMIC | | ■ | | ■ | ■ | |
| PA | | ■ | | ■ | ■ | |

Nota: Cinzento assinala a contribuição

**Fonte**: Adaptado de NATO e Rego (2015b, p.1.10-1.16, 2012, pp.4–7; 2016, pp.14–32)

# 4. A estrutura de planeamento, coordenação e sincronização de InfoOps ao nível Operacional

Neste capítulo iremos analisar a capacidade militar que está implementada no JFCBS e que permite a este Comando, planear, coordenar e integrar as InfoOps no plano operacional da Força. Será também analisado o contributo desta capacidade para a materialização das condições para atingir a SupInfo.

## 4.1. O Nível Operacional

A NATO (2017a, p.1.9-1.11) conduz as operações militares a três níveis distintos (Figura 18). O Estratégico-Militar, define o emprego da força armada ao abrigo da orientação política e como parte de uma estratégia coletiva com os restantes instrumentos de poder, de modo a atingir os objetivos estratégicos da Aliança. O nível Tático, é onde as Forças militares são empregues e conduzem tarefas militares na persecução de objetivos militares. E o nível Operacional, que sendo intermédio entre o Estratégico-Militar e o Tático, serve de ligação entre os dois. É a este nível que as campanhas são planeadas, conduzidas e sustentadas logisticamente de modo a atingir os objetivos estratégicos no Teatro de Operações. De igual modo, é ao nível Operacional que se combinam os resultados e efeitos das ações do nível Tático para atingir os objetivos estratégicos e o estado final desejado da campanha.

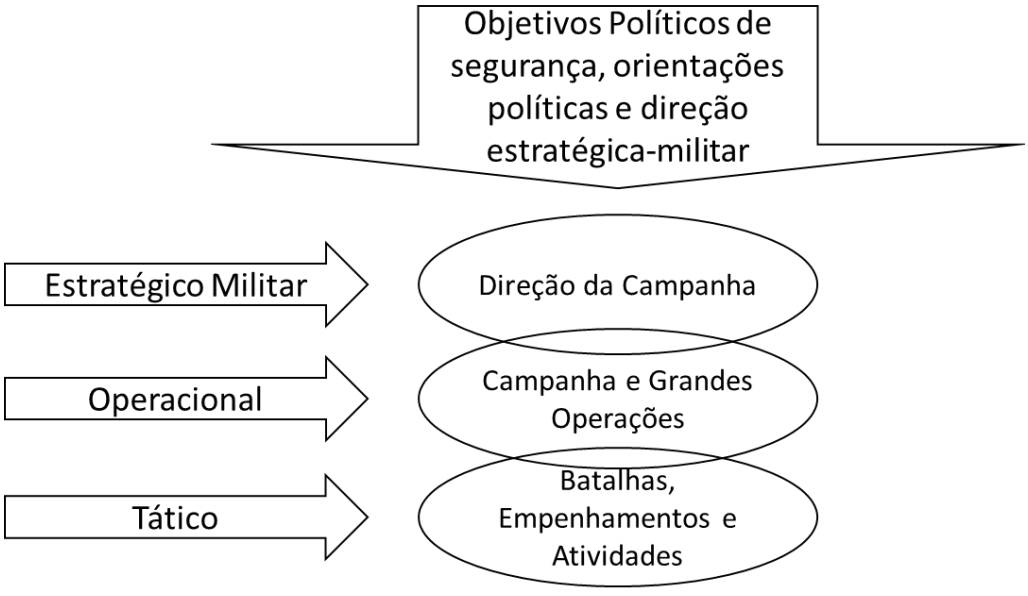



**Figura 18 - Os níveis das operações**

**Fonte**: Adaptado de NATO (2017a, p.1.9)

Nunes (2015c, p.190) refere "*O nível Operacional é por excelência o nível de planeamento onde se podem produzir ações capazes de moldar e intervir com eficácia no ambiente operacional, produzindo efeitos articulados e sincronizados*.". O mesmo autor

(2015c, pp.185–186), refere ainda que fruto da necessidade de moldar o AInfo, e considerando que todas as ações podem ter efeitos neste ambiente, a Informação constitui um instrumento de influência que intersecta várias áreas de atividade, não se restringindo ao domínio da Informação.

Nunes (2015c, pp.186–187), aponta quatro erros que decorrem de falta de integração de processos e da não consideração dos possíveis efeitos secundários das ações que se desenvolvem e que afetam o AInfo. Esses erros são:

- A falta de harmonização dos planos e das operações no domínio da informação;
- A não institucionalização dos processos de coordenação das atividades a desenvolver no domínio da informação;
- Decisores que desconhecem as opções disponíveis para afetar o AInfo e os sistemas de informação que suportam os processos de decisão;
- Falta de meios, métodos e treino para obter e manter uma adequada perceção da situação e desenvolver a compreensão do AInfo.

Entende-se assim, que se justifica a existência permanente num Comando de nível Operacional de um órgão com a responsabilidade de analisar o AInfo e de planear, avaliar e integrar as InfoOps no plano de campanha, de modo a que seja possível colmatar estes erros,

O JFCBS dispõe na sua organização de uma Secção de InfoOps. As principais responsabilidades desta Secção, são conduzir a avaliação do AInfo e aconselhar sobre e coordenar as todas as AI (Cinéticas/Não Cinéticas com as Letais/Não Letais) ao nível Operacional que afetam o AInfo (JFCBS, 2016, pp.2–3).

## 4.2. Doutrina

### 4.2.1. Enquadramento Doutrinário

Para a NATO a sua base doutrinária de InfoOps assenta nos seguintes manuais: "*MC422/4 NATO Military Policy on Information Operations*", "*AJP-3.10 Allied Joint Doctrine For Information Operations*" e o documento "*Bi-SC NATO InfoOps Reference Handbook*" (NATO IORH).

O MC422/4, destina-se a declarar a política militar da NATO para a implementação de InfoOps a todos os níveis da estrutura de comando da Aliança. Dá orientações para analisar e avaliar o AInfo e para conduzir o planeamento, a sincronização e avaliação das atividades que criam os efeitos desejados no AInfo. Nestas atividades incluem-se tarefas específicas aos Fogos e Manobra (NATO, 2012, p.3).

O AJP-3.10 é um documento doutrinário que tem como finalidade fornecer orientações

para integrar as InfoOps no planeamento, conduta e avaliação das Operações. Tem como base o MC422/4. O documento está orientado para o nível Operacional, no entanto, reconhece o papel da StratCom da Aliança como função que coordena as todas as atividades de comunicação. Este AJP, define e debate os princípios das InfoOps, destacando aqueles que em particular se consideram relevantes para a conduta das Operações. Nestes podem estar incluídos a sensibilidade aos fatores Políticos e ao papel de entidades não-militares (internas e externas à Aliança) e das capacidades que as tecnologias emergentes podem ter no AInfo (NATO, 2015b, p.ix).

O NATO IORH, fornece informação adicional que é necessária aos elementos de EM que conduzem o planeamento das InfoOps, de modo a que estes entendam e implementem a função integradora das InfoOps em todos os elementos da estrutura de Comando da Aliança. O documento abrange as experiências e as lições aprendidas, os procedimentos e técnicas empregues nas Operações em curso, bem como algum entendimento base para integrar a função InfoOps e os procedimentos no planeamento de OBE e na *Comprehensive Operations Planning Directive* (COPD) (NATO, 2010, p.3).

Koreman (2017), entende que o enquadramento doutrinário está adequado ao emprego das InfoOps na NATO e está alinhado entre si. Mesmo as Normas de Execução Permanente (NEP) em vigor nos JFC (Brunssum e Nápoles) estão sincronizadas entre si.

No entanto, é importante realçar que presentemente, há um desfasamento entre os documentos doutrinários. Com o AJP-3.10 na sua versão de 2015, torna-se necessário rever o NATO IORH, que está na sua versão de 2010.

#### 4.2.2. Processos

O enquadramento doutrinário define uma série de processos que permitem conduzir a análise do AInfo e integrar as AI no planeamento operacional. Define de igual modo, processos e metodologias para conduzir a avaliação das alterações provocadas no AInfo pelos efeitos produzidos.

##### 4.2.2.1. Planeamento

Segundo o AJP3-10 (NATO, 2015b, p.3.2-3.14) o planeamento das InfoOps é realizado concorrentemente com o desenvolvimento do OPLAN[38] durante os oito passos do processo de planeamento de nível Operacional (PPNO/OLPP) conforme prescrito na publicação doutrinária "*AJP-5 Allied Joint Doctrine for Operational-Level Planning*". No Anexo B, podemos observar o alinhamento dos passos, atividades e produtos que devem ser

[38] Plano de Operações ao Nível Operacional

elaborados pela Secção de InfoOps durante o OLPP.

O primeiro produto da Secção de InfoOps é a análise do AInfo. Esta é realizada nos passos 1 e 2 do OLPP e é executada segundo o modelo proposto pelo estudo de análise do AInfo (Anexo A do AJP-3.10). Como o próprio nome indica, destina-se a conduzir uma análise sistemática do AInfo em que as AI serão conduzidas durante a Campanha. Deve descrever os principais atores, os sistemas de informação disponíveis a esses atores e o ambiente mediático na AO. O estudo deve ser alvo de revisão constante, conforme as alterações no AInfo vão ocorrendo fruto das ações que sofre (NATO, 2015b, p.A.4; JFCBS, 2016, p.3; NATO, 2010, pp.15–19).

Na fase de planeamento os elementos da Secção que participam no *Joint Operational Planning Group* (JOPG) devem identificar os possíveis efeitos no AInfo e integrá-los no desenho operacional. Participam na análise PMESII[39], contribuindo de igual modo para a análise de fatores e identificação de centros de gravidade. É também durante esta fase que se identificam as MoE que serão usadas para avaliar os efeitos no AInfo durante o passo 8 do OLPP (JFCBS, 2016, p.4).

#### 4.2.2.2. Coordenação

A Coordenação das InfoOps é conduzida durante o passo 8 do OLPP, quando a operação está em execução. O processo usado para conduzir a coordenação é a *Information Activities Coordination Board* (IACB)[40]. Esta reunião faz parte do ritmo de batalha do JFC e é o principal processo para coordenar as AI no seio do JFC. Para além de analisar possíveis efeitos sobre o AInfo de ações conduzidas pelas restantes capacidades, deve coordenar as nomeações de possíveis alvos para a *Joint Targeting Coordination Board* (JTCB). A responsabilidade pela sua execução é do Chefe da Secção de InfoOps. A composição é variável, dependendo dos assuntos a discutir, sendo que a Figura 19 apresenta uma das possíveis propostas (NATO, 2015b, p.2.6-2.8; JFCBS, 2016, pp.3–4).

A IACB apoia o processo de avaliação revendo com regularidade as MoE relativas ao AInfo, sendo que pode ser necessário medir os efeitos diretos e indiretos, devendo sempre ter em consideração as consequências de possíveis efeitos indesejados (JFCBS, 2016, pp.3–4).

[39] Variáveis Operacionais (Politico, Militar, Económico, Social, Infraestruturas e Informação)
[40] A NEP do JFCBS ainda não está atualizada com a nova designação de *Information Activities Coordination Board* (IACB). O AJP-3-10 de referência ainda é a versão de 2009.

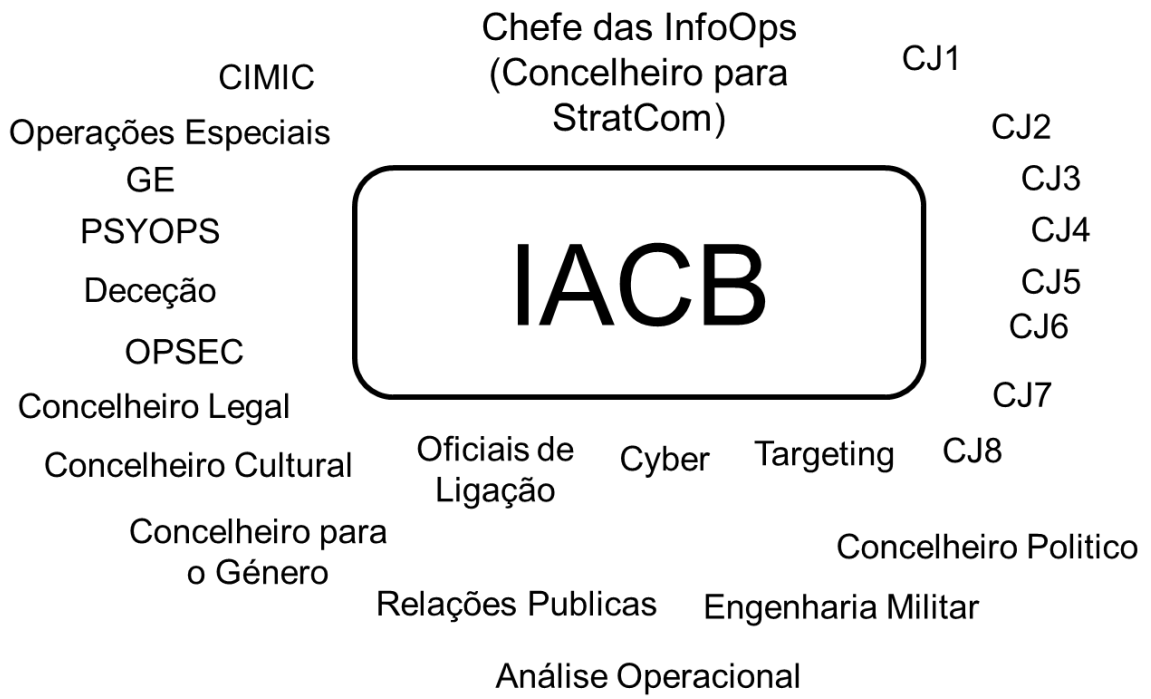



**Figura 19 - A IACB**

**Fonte**: NATO (2015b, p.2.6)

4.2.2.3. Integração

Para além da participação inicial no JOPG, a integração no OPLAN, é feita através da representação de um elemento da Secção de InfoOps na *Joint Coordination Board/Working Group* (JCB/JCWG) e na *Joint Targeting Coordination Board/Working Group* (JTCB/JTWG). Deve manter-se uma estreita coordenação com a JTCB/JTWG por forma a, tal como já foi referido, sejam tidas em conta no processo de *Targeting* as considerações em relação aos possíveis efeitos no AInfo das ações conduzidas (Koreman, 2017; JFCBS, 2016, pp.6–7, 2014a, p.9).

### 4.3. Organização e Pessoal

Iremos analisar a Organização em conjunto com o Pessoal. Sendo as organizações compostas por pessoas, estes dois vetores estão intimamente ligados entre si.

Doutrinariamente as AI devem ser planeadas sob a alçada do J5[41] e conduzidas sob a alçada dos J3[42] (NATO, 2015b, p.2.3). No JFCBS as InfoOps são responsabilidade da Secção de Efeitos e Influência, que além das InfoOps, englobam as PSYOPS. Esta célula está na dependência da Repartição de J3, da Divisão de Operações (Figura 20).

[41] Planos
[42] Operações

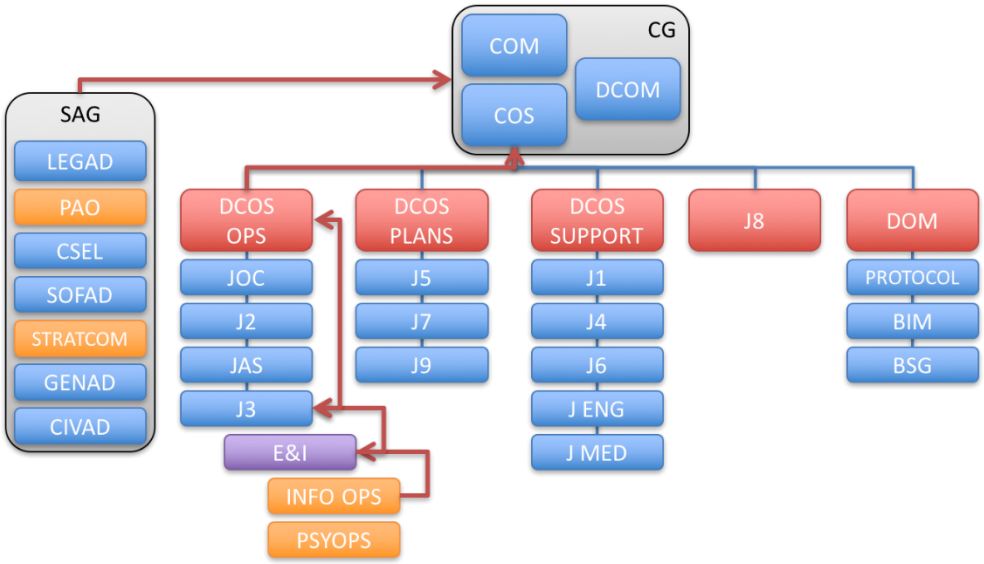



**Figura 20 - Inserção da Célula de InfoOps na Estrutura do JFCBS**

**Fonte**: Koreman (2017)

A Célula de InfoOps está organizada de acordo com a Figura 21. Podemos constatar que a sua organização está alinhada com a necessidade de Analisar, Planear, Avaliar e Integrar as AI nas Operações do JFCBS. A Análise e o Planeamento são conduzidos pela equipa de Planos, a Avaliação pela equipa com o mesmo nome e a Integração, pelas equipas de Sincronização, *Targeting*, *Engagement*, Consciência da Situação e Contra IED.

Este enquadramento organizacional está alinhado com o previsto na doutrina, promovendo e facilitando a coordenação do planeamento e sincronização das AI entre a Secção de InfoOps e o J5, J3 e o J2[43], uma vez que todas as Secções dependem do DCOS OPS.

O efetivo de PE[44] é de dezoito elementos, sendo dezassete Oficiais e um Sargento. Para efeitos de planeamento, não difere do quadro orgânico do CE[45]. Havendo necessidade de reforçar o efetivo, os elementos de reforço virão dos restantes Comandos da estrutura permanente da Aliança ou serão enviados pelas nações (Koreman, 2017).

[43] Informações
[44] PE – *Peace Establishment*: Quadro de pessoal dos QG da estrutura permanente da NATO em tempo de paz.
[45] CE – *Crisis Establishment*: Quadro de pessoal dos QG da estrutura permanente da NATO em tempo de crise.

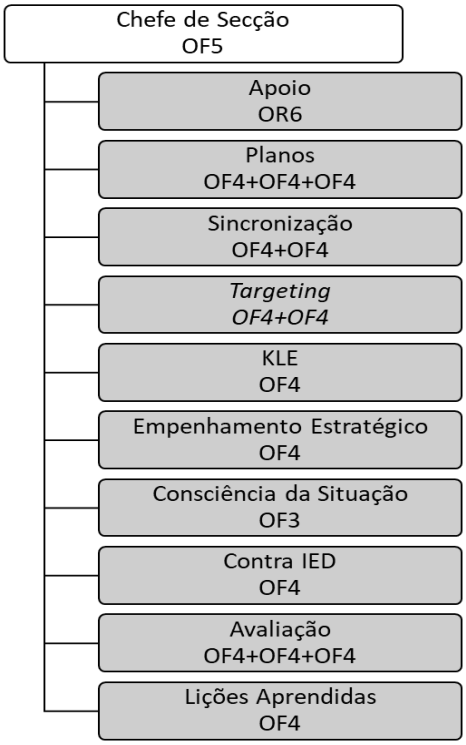



**Figura 21 - Organização da Secção de InfoOps**

**Fonte**: Koreman (2017)

### 4.4. Treino

A Aliança conduz exercícios militares para aprontar as suas Forças e EM, de modo a estarem prontas para responder aos atuais desafios de segurança. Os exercícios visam de igual modo, demonstrar as capacidades militares da Aliança e ajudar ao seu melhoramento (NATO, 2017b).

É a própria doutrina da Aliança que refere especificamente que as InfoOps devem ser integradas nos exercícios da Aliança. Assegura-se assim que os Comandantes e os seus EM compreendem o valor das InfoOps e das consequências negativas que advêm de não as empregar. A doutrina refere que os elementos de EM com funções de InfoOps devem ser envolvidos na conduta dos exercícios de modo a se poder retirar lições aprendidas (NATO, 2015b, p.4.1-4.2).

Segundo Koreman (2017), o FCCBS integra o planeamento das InfoOps em todas as atividades de treino em que participa, permitindo aos elementos da Secção e restantes elementos do EM, compreender como as InfoOps podem contribuir para atingir a SupInfo.

### 4.5. Material

A Aliança dispõe de uma rede informática que permite processar informação com classificação até NATO Secreto. Todos os sistemas funcionais e serviços informáticos da Aliança, estão suportados nesta rede.

No futuro, pretende-se implementar uma rede com capacidade "*plug-and-play*"[46], designada por NATO *Federated Mission Network* (FMN). Esta nova capacidade, permitirá a interligação de sensores, decisores e sistemas de armas, atingindo assim um dos desígnios das OCR que são a partilha de informação e a melhoria do processo de tomada de decisão (NATO, s.d., NCI Agency, 2014).

Para além da rede, importam os serviços que esta suporta, pois são esses que permitem dela retirar o seu pleno potencial. Alguns exemplos dos serviços disponíveis são, os Portais de *Sharepoint*™ que permitem a colaboração e a partilha de informação, *software* como o TOPFAS[47], MS Outlook/email, JCHAT[48] e MS Skype *for Businness*™, serviços de Vídeo Conferência[49] e o acesso à Internet (JFCBS, 2016, p.6; Koreman, 2017).

Koreman (2017), considera que as ferramentas disponíveis são suficientes para executar o planeamento, no entanto, refere que nem sempre são empregues da melhor maneira. Já a coordenação e a integração não dependem de ferramentas, mas sim de processos e da interação entre os participantes nos grupos de trabalho e das reuniões de coordenação, como é o caso das já referidas IACB e JCWG.

### 4.6. Liderança

Mais uma vez, a doutrina da Aliança refere explicitamente a necessidade de formação para os elementos que ocupem cargos relativos às InfoOps. Refere a necessidade de estar detalhada a descrição do cargo, de modo a que o elemento que ocupe a posição tenha clara consciência das suas responsabilidades. A necessidade de formação é extensível aos próprios Comandantes (NATO, 2015b, p.4.1-4.2).

A escola NATO em Oberammergau ministra dois cursos específicos de InfoOps. São eles o NATO *Senior Officer Information Operations Course* (NSOIOC) e o NATO *Information Operations Course* (NIOC).

O NSOIOC tem a duração de uma semana e é destinado a Majores ou oficiais de posto superior. Tem como objetivo de curso, conferir aos Oficiais Superiores da Aliança a aplicação dos conceitos relativos à StratCom e InfoOps, garantindo a consistência e credibilidade da mensagem e a sua relação com as demais funções e capacidades de comunicações (NSO, 2017a).

Já o NIOC dura, duas semanas e é destinado a Oficiais (Alferes a Tenente-Coronel) e

[46] Ligar e Usar, termo usado para designar a interligação entre sistemas sem necessidade de configurações adicionais
[47] *Tools for Operations Planning Functional Area Services*
[48] Joint Chat: Serviço de mensagens instantâneas que corre sobre a rede classificada.
[49] Sobre rede classificada.

Sargentos (1SAR a SMOR) que ocupem cargos na estrutura da NATO ou nas nações, relativos ao planeamento de InfoOps. Tem como objetivo de curso, treinar e educar os formandos oriundos das nações e dos Comandos da Aliança nos conceitos essenciais para a condução de InfoOps. As sessões são conduzidas em sala de aula. Incluem exercícios de planeamento orientados por um mentor. Estes são conduzidos em forma de sindicato. O curso tem como objetivos específicos (NSO, 2017b):

- Dadas as referências doutrinárias, compreender a política, doutrina e os conceitos de InfoOps da NATO;
- Explicar as capacidades, funções, ferramentas e técnicas que apoiam as InfoOps;
- Dado um cenário, com exemplos históricos ou atuais do emprego das InfoOps, identificar deficiências no planeamento, oportunidades e requisitos;
- Dado um cenário, conduzir o planeamento das InfoOps ao nível Operacional e de acordo com as ferramentas de planeamento em uso.

Koreman (2017) considera que a liderança a nível Operacional, integra plenamente o planeamento das InfoOps no planeamento da campanha. Promove a partilha de informação entre os elementos do seu comando conjunto e com os restantes comandos da estrutura permanente de comando da Aliança.

### 4.7. Interoperabilidade

A interoperabilidade[50] e a comunalidade das InfoOps na Aliança é garantida através da normalização de procedimentos e ferramentas entre os seus Comandos e Forças. Como foi referido anteriormente, as NEP dos dois JFC estão alinhadas entre si, o que significa que qualquer elemento de uma Secção pode integrar a Secção de InfoOps do outro Comando ou dos Comandos subordinados. Mesmo a formação é ministrada de forma normalizada (Koreman, 2017).

A interoperabilidade é também garantida através das ferramentas anteriormente descritas. Uma vez que as ferramentas são as mesmas, um elemento treinado e proficiente na sua utilização, facilmente poderá reforçar a estrutura de outro Comando da Aliança.

A normalização contribui de igual modo para a interoperabilidade, permitindo a modularidade das redes que suportam a partilha de informação. A utilização de *standards* abertos para o desenvolvimento das novas capacidades, nomeadamente ao nível das comunicações e de troca de informação, permite que as redes sejam estendidas com a adição de novos elementos. Estes novos elementos, podem ser a rede de missão de uma das nações

[50] Apêndice B

aliadas, novos sensores que partilham informação, ou novas ferramentas informáticas que apoiam o processo de tomada de decisão (Palfreyman, 2014).

### 4.8. A Superioridade de Informação

Analisada a estrutura que permite ao Comando Operacional planear, coordenar e integrar as InfoOps nas operações, resta agora analisar como pode esta estrutura contribuir para atingir as condições que materializam a SupInfo conforme foram enunciadas na secção 2.3.

Assim relativamente à necessidade uma rede de sistemas interoperáveis, a Aliança dispõe de uma rede de informática que permite a troca de informação classificada. Esta rede é gerida pela NCI *Agency* e os elementos da Secção são utilizadores dos seus serviços. De referir que esta rede serve toda a estrutura de Comando da NATO, ligando decisores a sistemas de armas e a sensores.

Quanto ao pessoal competente e treinado que seja capaz de colaborar, partilhar e utilizar a informação corretamente, e ajustar o comportamento dos sistemas e os níveis de interoperabilidade, podemos constatar que há uma organização permanente, com um PE definido. Os elementos da estrutura recebem formação, conduzem atividades de treino e dispõem dos sistemas que lhes permitem partilhar e utilizar informação.

Relativamente aos níveis adequados de GIC, este é um processo que não depende da Secção de InfoOps. Na NATO está à responsabilidade da NCI Agency através do "*The Knowledge Management Plan*" (Santos, 2016, p.28). No entanto, os elementos da Secção, dispõem das ferramentas para implementarem processos internos de GIC, tais como a rede informática e os portais *Sharepoint*™, e estão abrangidos pelas políticas de GIC do JFC (JFCBS, 2016, p.6).

Os serviços de TI que permitam obter uma visão operacional partilhada e ferramentas que sejam rápidas e intuitivas e permitam manter um fluxo ininterrupto de Informação, também estão disponíveis através da rede anteriormente mencionada. Esta rede disponibiliza serviços de planeamento (TOPFAS) e de colaboração em tempo real (VTC, *Skype*, *Sharepoint*™). É de destacar, que devido à utilização de uma rede baseada em protocolos abertos, é fácil disponibilizar serviços adicionais conforme venham a ser necessários.

O planeamento e preparação é atingido através da condução do estudo do AInfo e da participação dos elementos da Secção no JOPG durante o OLPP. Também o processo da IACB permite integrar o planeamento e avaliar se os efeitos das AI no AInfo estão a ser atingidos. Ainda colaboram para atingir esta condição, a participação de um elemento da Secção nos processos da JCB/WG e no JTCB/WG. Nestes processos, as AI são sincronizadas

e integradas na condução da campanha e são considerados os possíveis impactos no AInfo das ações que estão a ser conduzidas pelas restantes funções conjuntas. Estes processos, permitem manter uma consciência situacional elevada e atingir a almejada sincronização de ações e de decisões conforme referido por Nunes (2017).

A integração vertical e horizontal de capacidades como o IVR acontece de igual modo com a participação de elementos de ligação da J2 e *Targeting* nos processos da IACB, bem como de um elemento da Secção na ICB/WG[51] e na JTCB/WG. As atribuições aos meios de IVR podem ser planeadas e coordenadas nestes processos. A informação obtida através dos meios é também partilhada durante as reuniões e na rede através das ferramentas de partilha de informação (JFCBS, 2014b, p.6).

Os procedimentos adequados de Garantia de Informação e de proteção das redes, são assegurados e implementados pela J2 Segurança e pela J6[52] em coordenação com a CSU[53] da NCI *Agency* que serve o JFC. Estas entidades asseguram que a rede implementa os controlos adequados de modo a assegurar a Garantia da Informação (NATO, 2014, p.7.7). No entanto, a IACB tem representantes da área Ciber, da J2 e da OPSEC, o que permite coordenar os controlos a implementar para proteger a nossa liberdade de ação no AInfo (NATO, 2015b, p.2.6).

Sendo as InfoOps uma função coordenadora, não dispõem de meios próprios para afetar o AInfo. A condição de ter a capacidade de explorar ou negar ao adversário a utilização do AInfo é planeada, coordenada e integrada durante os processos acima descritos, nomeadamente durante a IACB/WG e a JTCB/WG. O primeiro passo para atingir esta condição é a execução criteriosa do estudo de Avaliação do AInfo. Só assim de pode compreender a natureza do adversário que enfrentamos e o uso que este faz do AInfo. Os processos implementados, permitem planear, coordenar e integrar as AI que serão desencadeadas de modo a negar ao adversário o uso do AInfo e a explorar a essa incapacidade, convertendo-a em oportunidades para a nossa Força. Aqui, realça-se a importância de se estabelecerem MoE exequíveis e mensuráveis de modo a se poder avaliar as alterações provocadas no AInfo.

Koreman (2017) considera que as InfoOps contribuiem para alcançar a SupInfo, no entanto, aponta dificuldades uma vez que é da opinião de que o conceito de SupInfo deveria ser revisto. Considera que atingir a SupInfo não é possível no atual quadro da conflitualidade

[51] *Intelligence Coordination Board/Working Group*
[52] Computers and Information Systems
[53] CIS Service Unit.

e tal como referem Nunes (2017), Koreman (2017) e o UK MoD (2013), a SupInfo, não é um fim em si, mas um meio para atingir uma consciência partilhada e um alinhamento procedimental e cognitivo.

## Conclusões

Na investigação desenvolvida, recorremos uma estratégia de investigação qualitativa onde através de um Estudo de Caso, analisámos a capacidade militar edificada no JFCBS que permite a este Comando, planear, coordenar e integrar as InfoOps nas suas operações. Procurámos também determinar como esta capacidade, analisada segundo o modelo dos vetores de desenvolvimento de uma capacidade militar, contribui para que as condições que permitem atingir a SupInfo sejam satisfeitas. Para tal, recorremos a uma revisão de literatura que assentou na doutrina e em documentos internos da Secção de InfoOps do JFCBS, recorrendo também a entrevistas com elementos que prestam serviço no referido Comando.

Vimos ao longo do segundo capítulo, como as OCR, o ciclo de Boyd e a SupInfo se interligam. O ciclo de OODA, é o processo que está na base da tomada de decisão dos atores do AInfo. Torna-se assim essencial proteger o nosso processo de tomada de decisão das ações do adversário e, consequentemente, afetar o seu processo de tomada de decisão.

Conduzir OCR tem como valor acrescentado a produção de melhores efeitos. Estes só podem ser garantidos através da obtenção de um estado de SupInfo. Ao conduzir atividades que procuram degradar a capacidade do adversário em avaliar a situação, estamos a criar a necessidade constante deste reavaliar a situação, logo de Observar e Orientar todo o seu processo de decisão. Aumenta-se assim, a necessidade de informação do adversário, pelo que, estamos a criar as condições para obter uma situação de SupInfo. Em consequência, o adversário fica impossibilitado de Decidir e Agir. Estamos assim em condições de responder à QD1 (Qual é o valor acrescentado de se conduzirem OCR?), atingindo o OE1 (Descrever a cadeia de valor das OCR).

Por seu lado, preservar a nossa capacidade de tomar decisões, protegendo as nossas redes e processos de gestão da Informação e melhorar o processo de reunião, processamento e disseminação da informação, contribui de igual modo para obter uma posição de SupInfo. Deste modo, preservamos e potenciamos assim, a nossa capacidade de conduzir as fases Observar e Orientar do ciclo de decisão. Criam-se assim condições para a efetiva tomada de Decisão e potenciação dos efeitos das Ações conduzidas. Ao elencar as condições para se obter a SupInfo (parágrafo 2.3.3, pág. 4), estamos em condições para responder à QD2 (Como se atinge a SupInfo?), atingindo o OE2 (Descrever como se atinge a SupInfo).

No terceiro capítulo, começámos por caracterizar o AInfo nos seus três domínios e seis camadas. Estabeleceu-se o paralelo com os domínios chave das OCR anteriormente descritos. Seguidamente, foram descritas as OBE, onde pudemos constatar como estas têm por objetivo afetar a vontade e o processo de tomada de decisão do adversário. Este objetivo

é conseguido através da produção de efeitos de um modo coordenado e encadeado sobre nós críticos de um sistema. Sendo os efeitos físicos produzidos sobre os nós críticos, de 1ª ordem, os que se produzem no domínio cognitivo, são designados de 2ª ordem e atuam sobre as perceções e vontade do adversário. Por seu lado, o encadeamento de ações, tem um efeito cumulativo no sistema. As OBE são potenciadas pelas OCR, como tínhamos visto no Capítulo 2, por estas últimas permitirem a produção de melhores efeitos.

Seguidamente, foi caracterizada a GI, este conceito tem por base a condução de operações militares no domínio da Informação. Estas operações apresentam aspetos complementares que visam explorar a informação disponível, proteger a nossa informação e ganhar a batalha das perceções. Estabelece-se o paralelo com as InfoOps, quando se constata que estas últimas são a condução da GI aos níveis Estratégico-Militar e Operacional. No entanto, ao nível tático, é conduzida a C2W.

Foram caracterizadas as InfoOps, descrevendo inicialmente como as AI são desenvolvidas para criar os efeitos desejados na Vontade, Compreensão e Capacidade dos adversários ou potenciais adversários e AA aprovadas em apoio aos objetivos de missão da Aliança. Estas não são uma capacidade em si, mas integram um conjunto de capacidades, fornecendo ao Comandante os meios para analisar, planear, avaliar e integrar as AI. Conclui-se assim da importância de existir ao nível Operacional, a capacidade militar para executar as funções descritas.

As capacidades e técnicas das InfoOps, foram descritas de modo a se poder determinar qual o seu produto para as Atividade Relacionadas e para a Finalidade das InfoOps. Apresentada a Tabela resumo (Tabela 1), respondemos assim à QD3 (Qual é o produto das capacidade e técnicas das InfoOps?) o que, nos permitiu atingir o OE3 (Descrever o conceito de InfoOps e qual o produto das suas Capacidades e Técnicas).

No quarto capítulo, começou-se por enquadrar a necessidade da existência da capacidade de planear, coordenar e integrar as InfoOps ao nível Operacional. Para tal descreveu-se o nível Operacional. Constatou-se que é neste nível das operações que se planeiam a sequência de condições, efeitos e ações que irão levar a atingir os objetivos estratégicos da campanha.

Seguidamente, foi analisada à luz dos vetores de desenvolvimento de uma capacidade militar, a estrutura que permite planear, coordenar e integrar as InfoOps ao nível de um comando operacional da NATO. Verificou-se que de facto, a estrutura pode ser descrita de acordo com os referidos vetores. Há uma doutrina que enquadra o seu emprego, bem como estão implementados os processos que permitem aos elementos desta estrutura, planear,

coordenar e integrar o planeamento das InfoOps nas operações da Força.

De igual modo, a estrutura tem uma organização funcional definida e está provida do pessoal com as competências e qualificações necessárias para desempenhar as suas funções.

São conduzidas ações de treino que visam a prática dos procedimentos e processos implementados quer ao nível da estrutura analisada, quer ao nível do comando.

Quanto ao vetor Material, a estrutura dispõe de redes e de serviços disponibilizados nessas redes, que suportam os processos implementados, a partilha de informação e a tomada de decisão, contribuindo assim, para uma visão partilhada da situação e para uma superioridade de decisão sobre um adversário.

Relativamente à Liderança, esta entende o contributo das InfoOps para a SupInfo e integra esta função nas operações da Força. Há cursos de formação para os elementos que integram a estrutura, bem como para os decisores que comandam as operações.

A normalização de processos, ferramentas e formação, permite atingir a Interoperabilidade entre estruturas semelhantes noutras organizações da Aliança, bem como com outras forças. Uma rede baseada em padrões abertos, que pode ser estendida e ligada a novas redes, é outro fator que colabora para se obter a interoperabilidade.

Considera-se assim que a H4.1 (A capacidade militar analisada está organizada segundo os vetores de desenvolvimento de uma capacidade) foi validada, o que permite responder afirmativamente à QD4 (Existe uma capacidade militar ao nível Operacional que permite planear, coordenar e integrar as diferentes capacidades de InfoOps?). Atingimos assim o OE4 (Identificar a Capacidade Militar ao nível Operacional que permite planear, coordenar e integrar as diferentes capacidades de InfoOps).

Neste capítulo podemos ainda verificar como a capacidade militar analisada contribui para que o JFC atinja a SupInfo satisfazendo as condições que permitem atingir a SupInfo. Para cada uma das condições, foi analisado o contributo de cada um dos vetores de desenvolvimento, verificando que todas elas podem ser atingidas. Nem todas as condições são satisfeitas diretamente por meios ou processos controlados pela Secção de InfoOps. No entanto, nos casos em que tal acontece, os meios e processos estão ao dispor da Secção para que deles se tire partido. Assim, validamos a H5.1 (A capacidade militar analisada permite satisfazer as condições necessárias para se atingir a SupInfo), o que nos permite responder à QD5 (Como é que a capacidade militar analisada contribui para a superioridade da informação?). A capacidade militar analisada, contribui para se atingir a SupInfo satisfazendo as condições que a materializam. Isto é conseguido através da implementação de processos que permitem planear, coordenar e integrar as AI conduzidas pelas capacidades

e técnicas das InfoOps, nas operações da Força e conjugar os seus efeitos com os produzidos pelas outras funções operacionais. Estes processos, incluem a avaliação dos efeitos e as alterações que as AI produzem no AInfo. Os efeitos não intencionais ou adversos, são também eles tidos em consideração. A integração da avaliação, permite introduzir mudanças e adaptar o OPLAN de modo a incorporar as referidas alterações do AInfo e do Espaço de Batalha. Isto conduz à capacidade de a Força amiga se adaptar e reagir ou induzir a mudança no AInfo e permite afetar o ciclo de decisão do adversário, levando assim à superioridade de decisão sobre este.

Consideramos assim que o OE5 (Compreender como a capacidade militar analisada contribui para a superioridade da informação) foi atingido.

Com a resposta às QD apresentadas, consideramos ter respondido à Questão Central, (Qual a capacidade militar edificada ao nível Operacional para planear, coordenar e integrar o emprego das capacidades e técnicas das InfoOps e de que modo contribui para a atingir a SupInfo?) tendo assim atingido o Objetivo Geral de investigação (No quadro das InfoOps, analisar a capacidade militar edificada ao nível Operacional para planear, coordenar e integrar o emprego das capacidades e técnicas das InfoOps e de que modo contribui para a atingir a SupInfo)

Este estudo identificou as condições que são necessárias atingir para se obter a SupInfo. Estas não estavam claramente descritas na doutrina ou na bibliografia consultada, pelo que foi necessário proceder à sua sistematização. Outro contributo para o desenvolvimento de conhecimento foi a descrição da estrutura de InfoOps ao nível Operacional. Analisar esta segundo os vetores de desenvolvimento de uma capacidade militar, permite compreender como se poderá implementar uma estrutura semelhante nas FFAA Nacionais.

Sendo este um Estudo de Caso, a principal limitação foi não se poder ter recorrido a uma técnica de observação direta sobre o objeto de estudo. Poder observar presencialmente os elementos da Secção de InfoOps a conduzir as suas atividades, teria permitido uma melhor compreensão dos processos e como estes contribuem para atingir a SupInfo.

Em estudos futuros no âmbito das InfoOps e em consequência deste estudo, seria interessante analisar a adaptação de uma estrutura equivalente à analisada, nas FFAA Nacionais.

**Bibliografia**


Alberts, D.S., Garstka, J.J. and Stein, F.P., 1999. *NETWORK CENTRIC WARFARE: Developing and Leveraging Information Superiority*. 2ª ed. CCRP Publications.

Ashley, M., 2012. KWar: Guerra Cibernética e Epistemológica. *Air&Space Power Journal*, (3), pp.72–88.

Autor, 2017. *Variação da posição dos oponentes no Domínio da Informação*. [Digital].

Curts, R., PhD and Frizzell, J., PhD, 2005. *Implementing Network Centric Command and Control*. [online] Available at: <http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/004.pdf>.

Department of Defense, 2005. *The Implementation of Network-Centric Warfare*. 1st ed. Washington DC: DIANE Publishing.

Dinis, J.A.H., 2005. *GUERRA DE INFORMAÇÃO – Perspectivas de Segurança e Competitividade*. 1st ed. Lisboa: Silabo.

MDN, 2014. Diretiva Ministerial de Planeamento de Defesa Militar (11400/2014). Lisboa: 2a Série. 175. DR.

EME, 2011. *Superioridade de Informação: Um Objectivo Estratégico para o Exército*.

EME, 2013. *NORMAS DE GESTÃO DE PROJETOS DO EXÉRCITO*.

IDN, 2013. *Estratégia da Informação e Segurança no Ciberespaço*. 1st ed. Cadernos IDN. [online] Lisboa: Instituto da Defesa Nacional. Available at: <http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf> [Accessed 15 Mar. 2017].

JFCBS, 2014a. *JTF HQ SOI 007.02 Joint Coordination Working Group*.

JFCBS, 2014b. *JTF HQ SOI 007.17 Intelligence Coordination Board/Working Group*.

JFCBS, 2016. *JTF HQ SOP 225 Information Operations*.

Koreman, L., 2017. *A capacidade militar de planeamento de Info Ops implementada no JFCBS*. 10 May.

Martins, J., 2016a. *A 'Cebola' da Investigação*. [Digital].

Martins, J., 2016b. *Corpo de Conceitos*. [Digital].

Martins, J., 2016c. *Percurso metodológico*. [Digital].

Martins, J., 2016d. *Plano geral de Investigação*. [Digital].

Moller, H.H., 2014. Effect-Based Thinking in NATO, Utilizing All Instruments of Power while Planning for and Conducting Operations. In: *Strategy in nato: preparing for an imperfect world.*, Palgrave Studies in Governance, Security, and Development. Dinamarca: Palgrave Macmillan, pp.173–189.

NATO, s.d. *Federated Mission Networking*. [online] http://www.act.nato.int. Available at: <http://www.act.nato.int/fmn> [Accessed 25 May 2017].

NATO, 2010. *Bi-SC NATO Information Operations Reference Book*.

NATO, 2012. *MC 0422/4 NATO Military Policy on Information Operations*.

NATO, 2013a. *AJP-5 Allied Joint Doctrine for Operational Level Planning*. AJP. Bruxelas: NSO.

NATO, 2013b. *Comprehensive Operations Planning Directive V2.0*. Bruxelas.

NATO, 2013c. *Secretary General's Annual Report 2012*. [online] NATO. Available at: <http://www.nato.int/cps/en/natohq/opinions_94220.htm> [Accessed 9 Dec. 2016].

NATO, 2014. *AJP-2 Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*. AJP. Bruxelas.

NATO, 2015a. *AAP-06 NATO GLOSSARY OF TERMS AND DEFINITIONS*. 1st ed. Bruxelas: NSO.

NATO, 2015b. *AJP-3.10 ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS*. 1st ed. NATO STANDARD. Bruxelas: NSO.

NATO, 2015c. *NATO Network Enabled Capability (NNEC) (archived)*. [online] NATO. Available at: <http://www.nato.int/cps/en/natohq/topics_54644.htm> [Accessed 10 Dec. 2016].

NATO, 2016. *North Atlantic Council (NAC)*. [online] NATO. Available at: <http://www.nato.int/cps/en/natohq/topics_49763.htm> [Accessed 9 Dec. 2016].

NATO, 2017a. *AJP-1 Allied Joint Doctrine*. Edition E Version 1 ed. NATO Standardization Office.

NATO, 2017b. *SHAPE | Exercises & Training*. [online] http://www.shape.nato.int. Available at: <http://www.shape.nato.int/exercises> [Accessed 25 May 2017].

NCI Agency, 2014, NATO Federated Mission Networking - effective information sharing during NATO Operations. [Video em linha] Bruxelas. Disponível em: <https://www.youtube.com/watch?v=f2PGinsYAi4> [Acedido 25 Mai. 2017].

NSO, 2017a. *N3-16 NATO Senior Officer Information Operations Course*. [online] NATO School. Available at: <http://www.natoschool.nato.int/Academics/Resident-Courses/Course-Catalogue/Course-description?ID=17&TabId=155&language=en-US#17aid-aid> [Accessed 9 May 2017].

NSO, 2017b. *N3-19 NATO Information Operations Course*. [online] NATO School. Available at: <http://www.natoschool.nato.int/Academics/Resident-Courses/Course-Catalogue/Course-description?ID=20&TabId=155&language=en-US#20aid-aid> [Accessed 9 May 2017].

Nunes, P.V., 2015a. *Guerra Baseada em Informações*.

Nunes, P.V., 2015b. *Information Superiority e Net Centric Warfare*.

Nunes, P.V., 2015c. *Sociedade em rede, ciberespacço e guerra de informacão: contributos para o enquadramento e construção de uma estratégia nacional da informação*. 2ª ed. Lisboa: Atena.

Nunes, P.V., 2017. *Validação das Condições para a Superioridade e Informação*. 28 May.

Conselho de Ministros, 2014. Orgânica do EMGFA (DL 184/2014). Lisboa: 1a Serie. 250. DR.

Osinga, F.P.B., 2005. *Science, Strategy and War: The Strategic Theory of John Boyd*. 1st ed. Amsterdam: Eburon Academic Publishers.

Palaganas, R., 2007. Implementing Nato Network Enabled Capability: implications for Nato Response Force's envisioned roles. *Information as Power*, 1, pp.175–197.

Palfreyman, J., 2014. *NATO Federated Mission Networking*. [online] IBM Government Industry Blog. Available at: <https://www.ibm.com/blogs/insights-on-business/government/nato-federated-mission-networking/> [Accessed 25 May 2017].

Radenović, S., s.d. Observe-Orient-Decide-Act (OODA) by John Boyd. [online] Available at: <https://www.academia.edu/8347535/Observe-Orient-Decide-Act_OODA_by_John_Boyd> [Accessed 29 Jan. 2017].

Randall, B., 2001. *Sun Tzu: The art of Network Centric Warfare*. [online] US Army War College. Available at: <http://handle.dtic.mil/100.2/ADA389680> [Accessed 14 Jul. 2015].

Rego, N., 2016. *OC 4.2 Operações de Informação*.

Rego, N., 2017. *EDO 25 Operações no Ciberespaço*.

Ribeiro, C.O., 2008. Guerra Centrada em rede: Um Conceito Operacional Emergente no Séc XXI. *Proelium*, pp.35–66.

Santos, P., 2016. *Gestão de Informação e do Conhecimento*. [online] Available at: <http://comum.rcaap.pt/handle/10400.26/14617> [Accessed 18 Nov. 2016].

Schechtman, G., 1996. *Manipulating The OODA Loop: The Overlooked Role of Information Resource Management In Information Warfare*. [Tese] Air University. Available at: <http://www.au.af.mil/au/awc/awcgate/afit/schec_gm.pdf> [Accessed 1 Feb. 2017].

Toffler, A. and Toffler, H., 1994. *Guerra e Antiguerra*. Translated by C. Tavares. Lisboa: Livros do Brasil.

UK MoD, 2013. *Joint Doctrine Note 2/13 Information Superiority*. Joint Doctrine. Swindon: UK MoD.

US ARMY, 2001. *FM 3-0 Operations*. Field Manual. Washington DC: US Army.

US ARMY, 2016. *Strategic Cyberspace Operations Guide*.

Vego, M.N., 2009. *Joint Operational Warfare: Theory and Practice*. Government Printing Office.

Vicente, J.P.N., 2006. Operações Baseadas em Efeitos: o Paradigma da Guerra do séc. XXI. *Nação e Defesa*, (114), pp.229–256.

Vicente, J.P.N., 2008. Operações em Rede: da promessa à realidade. *Nação e Defesa*, (120), pp.51–76.

# Anexo A - As Características e Princípios da Superioridade de Informação

**Tabela 2 - Características Permanentes da Superioridade de Informação**

| | |
|---|---|
| Liderada pelo Comando | A SupInfo não se consegue apenas por se ter as capacidades e os procedimentos apropriados implementados. Dependendo da situação, os comandantes devem desenvolver as suas próprias estratégias de modo a alcançar a SupInfo sobre os outros atores, dando-lhes a devida prioridade. |
| Competitiva | É necessário um esforço contínuo para alcançar e manter a SupInfo. A SupInfo não é absoluta e degradar-se-á ao longo do tempo. Também pode ser ativamente degradada pelas atividades de InfoOps dos nossos adversários ou diminuída pelas nossas próprias ações. |
| Comparativo | A condição de SupInfo apenas existe quando temos algum grau de diferença de *insight* e previsão sobre outrem. À medida que as assimetrias e o conhecimento mudam, também o grau de superioridade da informação alcançado varia. As mudanças podem ser provocadas pelas nossas próprias ações, por ações de terceiros, ou por efeitos mais amplos, como alterações climáticas. |
| Dependente do Contexto | O modo pelo qual a SupInfo é alcançada, é único para cada situação e relativa a cada conjunto de atores. Embora possam estar disponíveis (com base nos princípios enunciados) modelos para alcançar a SupInfo, estes devem ser adaptados às circunstâncias. |
| Muda ao longo do tempo | A SupInfo é um estado em mudança dinâmica que surge a partir dos comportamentos adaptativos das pessoas e do seu uso de sistemas de informação ao longo do tempo. O grau e a natureza da SupInfo está sempre em constante mudança, não há objetivo ou estado final. De modo análogo à capacidade ciber, as capacidades em que a SupInfo é construída evoluem continuamente, a par das inovações na tecnologia. Portanto, as formas como alcançamos a SupInfo mudarão no futuro. |

**Fonte**: UK MoD (2013, p.1.5-1.6)

**Tabela 3 - Princípios da Superioridade de Informação**

| | |
|---|---|
| Princípio 1 | SupInfo é mais do que apenas negar informação ao nosso adversário. É praticamente impossível impedir o acesso os nossos adversários de acederem a informação. Os Comandantes podem até pretender fazer o oposto, fornecendo aos adversários informação que lhes faça ver a futilidade da sua posição, enganá-los ou torná-los dependentes da sua disponibilidade. |
| Princípio 2 | SupInfo envolve risco e compromisso. O grau de SupInfo que se possui vai ser difícil de avaliar. Isto deve-se à SupInfo ser relativa, transitória, subjetiva, inteligível e muito dependente do contexto e da personalidade. Desenvolver esforços para tentar saber o que pode não vir a ser sabido, pode ser fator de distração. Os Comandantes devem estar preparados para continuar, aceitando que a situação pode vir a ser clarificada mais tarde. Uma estratégia válida para quebrar o impasse, pode ser, desencadear uma ação de modo a estimular uma reação por parte dos outros atores. Haverá sempre um grau de risco que decorre da interpretação e do improviso necessários para aqueles que estão envolvidos no planeamento. Este decorre das oportunidades e ameaças em constantemente variáveis. |

| | |
|---|---|
| | Aguardar pela certeza, não é opção quando somos confrontados com uma situação de incerteza que pode levar a um choque estratégico. Em vez disso, o Comandante deve usar da sua capacidade de julgamento, de decisão e experiência para transformar o risco em oportunidade. |
| Princípio 3 | SupInfo é um estado que apoia a eficácia da Tomada de Decisão. A SupInfo é o capacitador da relação entre, Informações, a Compreensão e a Tomada de Decisão e fornece a vantagem informacional que é necessária para tomar decisões eficazes. Não é uma capacidade de *per si*. Só se pode atingira SupInfo quando os Comandantes podem decidir o modo como os sistemas de informação são configurados e empregues. Ter a capacidade de empregar e adaptar a situação de SupInfo, permite aos Comandantes alterarem o seu Compreensão e a sua Tomada de Decisão de acordo com o desenvolvimento dos imperativos operacionais. É mais fácil reconhecer o facto de não se dispor de SupInfo, do que quando se a tem. Por exemplo, quando um Comandante percebe que não consegue obter informação suficiente para tomar decisões atempadas, é evidente que não possui SupInfo. |
| Princípio 4 | A SupInfo tem aspetos ambientais. Alguma da vantagem no domínio da informação advém de explorar diferenças na geografia do terreno. Esta inclui a capacidade de analisar o tempo, o espaço e todos os ambientes operacionais. Por exemplo, para analisar o tempo, o Comandante deve poder explorar dados históricos para identificar padrões de comportamento que possam levar a perceber intenções futuras e tendências de comportamento da ameaça, o que leva à SupInfo. |
| Princípio 5 | O carácter da SupInfo altera-se. A SupInfo sempre esteve presente na conflitualidade, mas não é a mesma que foi ou virá a ser. No futuro, a SupInfo não se deverá somente a avanços tecnológicos, a sua dimensão humana será sempre um fator dominante. Para manter a vantagem competitiva, os Comandantes terão de adaptar as suas estratégias de SupInfo e atualizá-las à medida que a situação muda. |
| Princípio 6 | O grau de SupInfo que pode ser conseguido, pode ser influenciado direta, ou indiretamente. A SupInfo é fator intangível do potencial de combate, tal como a moral. No entanto, pode ser ajustada de várias maneiras de modo a alterar a vantagem relativa a outros atores. Na maior parte das circunstâncias necessitará de uma influência direta ou indireta, devendo-se ter em conta que os outros atores e o ambiente mais alargado também exercerão a sua influência. O Comandante deve avaliar esta complexidade de interligações e de efeitos (muitos dos quais não são visíveis) na sua situação de informação. |
| Princípio 7 | A SupInfo é uma vantagem relativa. Esta vantagem pode ser relativa a outros atores, relativa à nossa capacidade de corresponder às exigências e imperativos da situação, e é afetada pelo modo como os atores são capazes de avaliar essa vantagem relativa. |

**Fonte**: Uk MoD (2013, p.1.7-1.9)

## Anexo B – Planeamento das InfoOps

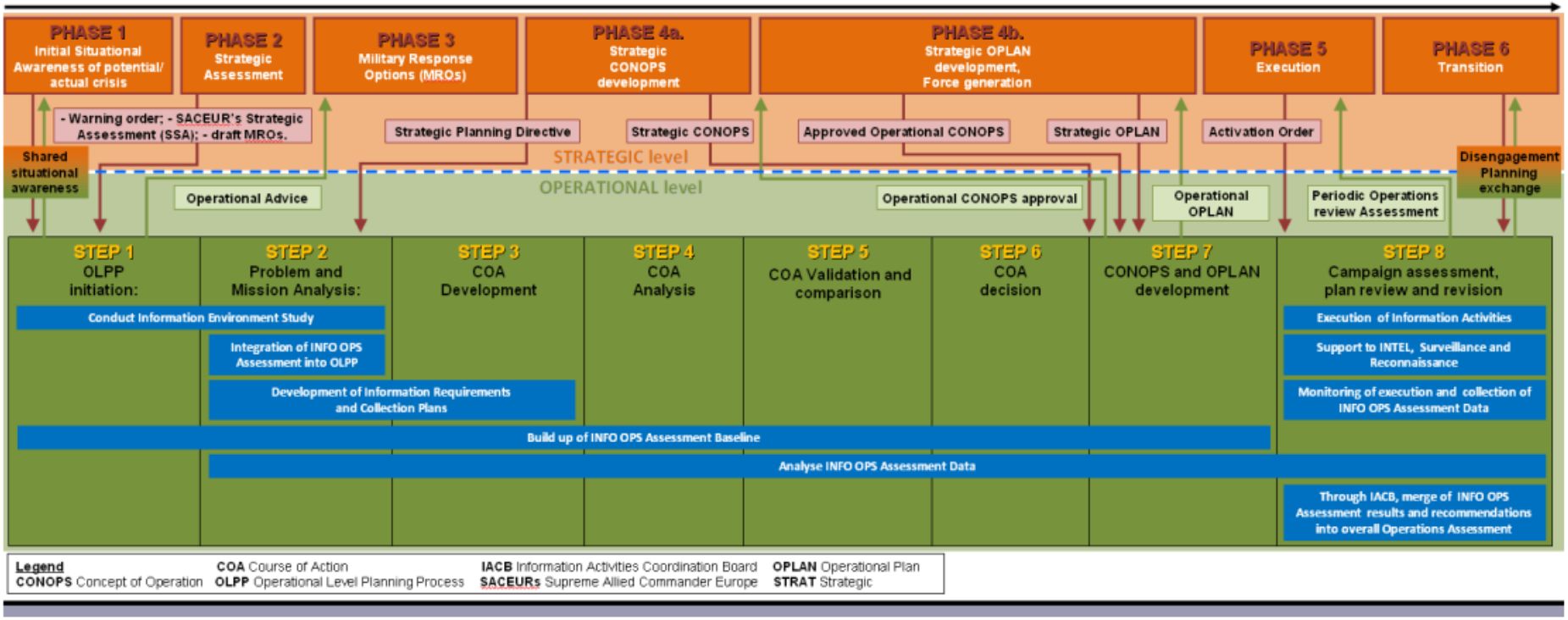



**Figura 22 - Atividades de Planeamento das InfoOps e seus produtos**

**Fonte**: NATO (2015b, p.3.13)

# Apêndice A - Tabelas complementares à metodologia

**Tabela 4 - Modelo de Análise**

<table>
<tr><td colspan="6">Objeto de Investigação: A capacidade militar edificada ao nível Operacional que permite planear, coordenar e integrar as capacidades e técnicas associadas às InfoOps</td></tr>
<tr><td colspan="6">Objetivo Geral: No quadro das InfoOps, analisar a capacidade militar edificada ao nível Operacional para planear, coordenar e integrar o emprego das capacidades e técnicas das InfoOps e de que modo contribuem para a atingir a SupInfo</td></tr>
<tr><td colspan="2" rowspan="2">Objetivos Específicos</td><td colspan="4">Questão Central: Qual a capacidade militar edificada ao nível Operacional para planear, coordenar e integrar o emprego das InfoOps e de que modo contribui para a atingir a SupInfo?</td></tr>
<tr><td colspan="2">Questões Derivadas</td><td>Conceitos</td><td>Dimensão</td></tr>
<tr><td>OE1</td><td>Descrever a cadeia de valor das OCR</td><td>QD1</td><td>Qual é o valor acrescentado de se conduzirem OCR?</td><td>OCR</td><td rowspan="2">Conceito de SupInfo</td></tr>
<tr><td>OE2</td><td>Descrever como se atinge a SupInfo</td><td>QD2</td><td>Como se atinge a SupInfo?</td><td>SupInfo</td></tr>
<tr><td>OE3</td><td>Descrever o conceito de InfoOps e qual o produto das suas Capacidades e Técnicas.</td><td>QD3</td><td>Qual é o produto das capacidade e técnicas das InfoOps?</td><td>InfoOps</td><td>Conceito de InfoOps</td></tr>
<tr><td>OE4</td><td>Identificar a Capacidade Militar ao nível Operacional que permite planear, coordenar e integrar as diferentes atividades de InfoOps.</td><td>QD4</td><td>Existe uma capacidade militar ao nível Operacional que permite planear, coordenar e integrar as diferentes atividades de InfoOps?</td><td>Capacidade Militar</td><td rowspan="2">Capacidade Militar edificada ao nível Operacional que permite planear, coordenar integrar as diferentes capacidade e técnicas das InfoOps</td></tr>
<tr><td>OE5</td><td>Compreender como a capacidade militar analisada contribui para a superioridade da informação</td><td>QD5</td><td>Como é que a capacidade militar analisada contribui para a superioridade da informação?</td><td>Contributo da Capacidade Militar para a SupInfo</td></tr>
</table>

**Tabela 5 – Indicadores que confirmam as hipóteses**

| Conceito | Dimensão | Hipótese | Indicador |
|---|---|---|---|
| Capacidade Militar | Doutrina | H4.1 | • Presença de um quadro doutrinário que conceptualiza o planeamento das InfoOps.<br>• Quadro doutrinário permite a compreensão do contributo das InfoOps para a SupInfo.<br>• Existência de Processos de planeamentos, coordenação e sincronização das InfoOps. |
| | Organização | | • Existência de uma organização permanente com a responsabilidade do planeamento de InfoOps. |
| | Treino | | • O Comando inclui o planeamento de InfoOps nos exercícios em que participa.<br>• O treino permite compreender o contributo das InfoOps para a SupInfo. |

| | | | |
|---|---|---|---|
| | Material | | • O órgão de planeamento tem ao seu dispor uma rede informática que lhe permite o trabalho em ambiente colaborativo em tempo real.<br>• O órgão de planeamento tem ao seu dispor as ferramentas informáticas (*Software*) que lhe permite planear, coordenar e integrar as diferentes capacidades e técnicas das InfoOps. |
| | Liderança | | • A Liderança integra as InfoOps no planeamento das operações.<br>• A Liderança promove a partilha de informação entre as diversas células do EM.<br>• A Liderança promove a partilha de informação com entidades externas e com as unidades subordinadas.<br>• O pessoal que compõe o órgão responsável pelo planeamento de InfoOps tem formação em planeamento de InfoOps. |
| | Pessoal | | • O órgão de planeamento de InfoOps tem pessoal atribuído na estrutura do PE.<br>• É previsto o órgão de planeamento de InfoOps ser aumentado na estrutura de CE.<br>• Durante um Crise/Exercício, o órgão de planeamento de InfoOps é aumentado com elementos vindos dos elementos que compõem as capacidades e técnicas das InfoOps. |
| | Infraestruturas | | • Sem indicador |
| | Interoperabili-dade | | • Os procedimentos e a formação permitem a permuta de elementos entre os Comandos da Aliança.<br>• Ferramentas/redes informáticas permitem a integração da informação partilhadas pelas várias capacidades e técnicas das InfoOps.<br>• A arquitetura da rede, permite a integração das redes de sensores, de informação e de combate. |
| Superioridade de Informação | Superioridade de Informação | H5.1 | • Os meios, os processos e as atividades desenvolvidas pela capacidade militar analisada permitem atingir as condições para a obtenção da SupInfo. |

## Apêndice B - Conceitos complementares

| | |
|---|---|
| Ação | Processo de empenhamento de um instrumento, na área de operações, de modo a criar um (ou vários) efeito(s) específico(s) na persecução de um objetivo (NATO, 2013b, p.3.26). |
| Ambiente de Informação | É composto pela informação propriamente dita, pelos indivíduos, organizações e sistemas que recebem, processam e transmitem informação. É o espaço cognitivo, virtual e físico em que tal ocorre. (NATO, 2012, p.B-1) |
| Ator (Atores) | O termo ator é usado no seu sentido mais lato ao longo deste documento. Inclui a liderança política, comandantes militares, indivíduos influentes, militares, fações armadas e grupos populacionais específicos (por exemplo, étnicos, culturais, religiosos e políticos). Os atores podem ser adversários, potenciais adversários ou outras audiências aprovadas pelo NAC (NATO, 2015b, p.1.7). |
| Centro de Gravidade | Características, capacidades ou locais a partir do qual deriva a liberdade de ação, a força física ou a vontade de lutar de uma nação, aliança, Força militar ou outro grupo (NATO, 2013a, p.2.32). |
| Comunalidade | O estado alcançado quando são empregues a mesma doutrina, procedimentos ou equipamentos (NATO, 2015a, p.2.C.9) |
| Doutrina (Vetor de Desenvolvimento) | Representa um conjunto de princípios e regras que visam orientar as ações das forças e elementos militares, na prossecução dos objetivos associados ao desenvolvimento de uma determinada capacidade. Compreende táticas, técnicas e procedimentos para conduzir tarefas (EME, 2013, p.11). |
| Efeito | Estado (físico ou comportamental) de um sistema que resulta de uma ação ou conjunto de ações desenvolvidas contra esse sistema, o objeto/entidade que sofre esse efeito pode ser visto como um nó de uma rede que, por sua vez, pode estabelecer interações com outros nós (Nunes, 2015c, p.199). |
| HUMINT | Uma categoria das Informações que deriva da informação recolhida a partir de fontes humanas. (NATO, 2015a, p.2.H.5) |
| Informação | Dados não processados, de qualquer natureza, que podem ser utilizados na produção de informações (NATO, 2015a). |
| *Information Assurance* | A *Information Assurance*, é o conjunto de atividades e medidas para proteger e defender a informação e os sistemas de informação, garantindo a sua disponibilidade, integridade, autenticidade, confidencialidade e não repudio. Estas medidas incluem a garantia de restauro dos sistemas de informação através da incorporação de capacidades de Proteção, Deteção de intrusão e de Reação. (US ARMY, 2016, p.102) |
| Infraestruturas (Vetor de Desenvolvimento) | Define todas as infraestruturas necessárias para alojar, treinar e aprontar forças, bem como operar e sustentar meios (e.g.: oficinas, centros de simulação, etc.) de acordo com uma determinada capacidade (EME, 2013, p.13). |
| Interoperabilidade (Vetor de Desenvolvimento) | Representa o processo colaborativo de planeamento e execução, destinado a alcançar e manter o nível de normalização e |

| | |
|---|---|
| | sincronização de todos os vetores associados ao desenvolvimento de uma determinada capacidade (EME, 2013, p.13). |
| Interoperabilidade | A capacidade de agir em conjunto de forma coerente, eficaz e eficiente para atingir objetivos táticos, operacionais e estratégicos (NATO, 2015a, p.2.I.8) |
| Interoperabilidade de Forças | A capacidade de forças de duas ou mais nações, para treinar, conduzirem exercícios e operar eficazmente em conjunto na execução das tarefas e missões atribuídas (NATO, 2015a, p.2.F.5) |
| Liderança (e Formação) (Vetor de Desenvolvimento) | Abrange as atividades de liderança e formação individual destinadas a conferir as competências necessárias ao desempenho de cargos específicos de acordo com uma determinada capacidade. É um processo de organização das situações de aprendizagem específicas cuja finalidade é conferir, desenvolver e/ou incutir capacidades (conhecimentos/aptidões/atitudes), para o desempenho de uma função específica. Compreende a Instrução Militar, Formação Contínua e Formação Profissional (EME, 2013, p.12). |
| Material (Vetor de Desenvolvimento) | Inclui todos os equipamentos, sobressalentes e tecnologia necessários para equipar, operar, manter e sustentar uma determinada capacidade (EME, 2013, p.12). |
| Organização (Vetor de Desenvolvimento) | Define as estruturas, forças e elementos militares necessários para operar, manter e sustentar uma determinada capacidade (EME, 2013, p.12). |
| Pessoal (Vetor de Desenvolvimento) | Representa o tipo e quantidade de recursos humanos necessários para operar, manter e sustentar uma determinada capacidade. Inclui a identificação de especialistas e/ou as competências necessárias (EME, 2013, p.12). |
| Sistemas de Informação | Conjunto de equipamentos, métodos e procedimentos e se necessário pessoal, organizado para desempenhar funções de processamento de informação (NATO, 2015a) |
| Superioridade de Decisão | O estado em que são tomadas e implementadas decisões melhor informadas e de um modo mais rápido do que o adversário se pode adaptar, permitindo ao Comandante da Força moldar o ambiente às suas necessidades e objetivos. Está dependente de se obter e manter um estado de SupInfo e de consciência situacional partilhada durante todas as fases da operação (Palaganas, 2007, p.179). |
| Tempo Operacional | Ritmo a que se desenrola a Campanha ou Operação. Quanto maior for o Tempo Operacional, maior será a iniciativa da Força que marca o ritmo das operações (Vego, 2009, p.IX.127). |
| Treino (Vetor de Desenvolvimento) | Define os processos de organização das situações de aprendizagem, através da aplicação prática e sistemática dos conhecimentos adquiridos e cuja finalidade é a manutenção e aperfeiçoamento dos conhecimentos/aptidões/atitudes previamente adquiridos, associados à aplicação/emprego de uma determinada capacidade. Inclui o Treino individual e Coletivo, nas vertentes do Treino na Função, Treino Orientado e Treino Operacional (EME, 2013, p.12). |

# Apêndice C - A Arquitetura das Operações Centradas em Rede

**Rede de Informação**

A Rede de Informação é a info-estrutura física que liga a Força e realiza o processamento, arquivo, difusão e proteção da informação. Esta é a rede que permite efetivamente obter a SupInfo, uma vez que serve de suporte às outras redes. É constituída por links de comunicações e redes de computadores que permitem a interligação de todas as Forças no Espaço de Batalha. Esta Rede de Informação deve ter implementados controlos de proteção e defesa que lhe permitam ter um elevado grau de resistência e resiliência a ataques. Para além da capacidade de proteção, deve também ter redundância e capacidade de garantir a continuidade de operação mesmo que, em modo degradado. (Ribeiro, 2008)

**Rede de Combate**

Esta rede recebe *inputs* da rede de informação para conduzir o planeamento e a execução das operações militares. Por vezes, há a necessidade dos sistemas de armas se ligarem diretamente à rede de sensores. Quando isto acontece, estabelece-se uma relação que se designa de *Sensor-to-Shooter*. A grande vantagem da Força em usar a Rede de Combate é a capacidade de partilhar uma visão comum da situação e muito mais rapidamente se adaptar às ações do adversário ou às alterações do Espaço de Batalha. Outra grande vantagem é a gestão integrada da Força. O Comandante tem mais facilidade em atribuir as tarefas às Unidades que encontrarem em melhores condições de as cumprir. Tem sempre um conhecimento atualizado do estado de prontidão de cada uma das Unidades ou sistemas que tem ao seu dispor. Esta gestão integrada também permite aumentar o ritmo da batalha, o que nos leva a conseguir moldar o ciclo de decisão do adversário (Ribeiro, 2008), levando-o à reação em oposição à nossa ação.

Esta rede pode ainda dividir-se em diversas sub-redes como são exemplo as redes táticas para a Artilharia de Campanha, para a Defesa Aérea ou para o comando da manobra como é o caso do FBCB2[54].

**Rede de Sensores**

A Rede de Sensores permite ao Comandante recolher a informação sobre o Espaço de Batalha. Esta rede alimenta a rede de informação com os dados recolhidos pelos sensores. Ao dispor de uma visão atualizada, mais próxima possível do tempo real, o Comandante da Força está em condições de tomar a decisão correta e levar o adversário a reagir em vez de lhe permitir tomar a iniciativa do desenvolvimento das suas ações (Ribeiro, 2008).

A grande vantagem destas redes é que a informação dos sensores pode chegar a qualquer um dos escalões. Há uma partilha imediata da informação sobre a qual se podem tomar decisões. Como foi referido anteriormente, os elementos de informação referentes à aquisição de objetivos podem inclusivamente ser imediatamente enviados para o sistema de armas que irá produzir efeitos no objetivo. O posterior tratamento destes dados é efetuado pela Rede de Informação.

[54] Force XXI Battle Command Brigade and Below.

## Apêndice D – Entrevistas

Entrevistado: Coronel Tms Paulo Viegas Nunes.

Local: Academia Militar, Amadora

Data: 28abr2017

### 1. Condições para obter a Superioridade de Informação

1.1 Podemos falar em condições decisivas para se obter a Superioridade de Informação? Se sim, quais são?

Concorda as Condições elencadas (Parágrafo 2.3.3).

"A Superioridade de Informação é um "*Way*" e não um "*End*".

Refere:

"Todas as condições apresentadas são do domínio físico e Informação. Não há nenhuma que seja no domínio Cognitivo".

Entrevistador: Não considera que o pessoal competente treinado seja uma condição do domínio Cognitivo?

"É muito pouco, pode ser considerado medidas de eficiência e eficácia?

Como Condições no domínio Cognitivo refere:

"Consciência partilhada. O treino há-de criar identidade de raciocínio, aplicar os mesmos métodos criando metodologias comuns, mas depois é a fusão da informação que vai permitir que, não só as metodologias como aquilo que é a visão, produza decisões alinhas. Podemos treinar, mas se não tivermos os mesmos métodos de decisão, as decisões podem desalinhar. Aí o que se fala é isso mesmo, alinhamento procedimental e cognitivo."

1.2 Como pode um ator reconhecer a sua posição de superioridade no domínio da informação?

"A maturidade de informação, não é fácil de medir. É preciso criar métricas e indicadores e esses indicadores e métricas não são sempre iguais, são dependentes da própria missão, da circunstância, do tempo disponível, são dependentes de uma série de varáveis que têm de ser consideradas. Nós só podemos comparar para a mesma missão, com as mesmas variáveis."

### 2. A Função integradora de EM InfoOps

2.1 De que modo função integradora de EM InfoOps, pode contribuir para a obtenção da Superioridade de Informação?

"Através da implementação de processos e métodos. É preciso ainda estabelecer as métricas, Medidas de Eficácia e Medidas de Desempenho"

Entrevistado: OF4 DEU (A) Lars Koreman

Entrevista por Email

Data: 10mai2017

**Disclaimer** - The views expressed in this expert interview and subsequent comments and explanations are those of the LtCol (OF-4) DEU Army Lars Koreman and do not necessarily reflect the official position of NATO, HQ Joint Force Command Brunssum or the German Armed Forces.

**1. Doctrine**

**Q:** Does NATO InfoOps Doctrinal Framework properly conceptualize the employment of InfoOps in support of Military Operations? Is there the need for additional Doctrine or SOP?

**KOR**: The INFOOPS doctrine (AJP 3.10) properly conceptualises the employment of INFOOPS in support of military operations and is fully in line with the respective InfoOps policy. The doctrine is fully in line with the StratCom policy and synchronised with the PSYOPS doctrine (AJP 3.10.1). Unfortunately, there is no PAO doctrine, only a policy and a handbook. InfoOps, PSYOPS and PAO are defined as the military communication capabilities and staff functions, working under the umbrella/framework of StratCom. The SOPs are synchronised and implemented by both operational HQs, JFC Brunssum and JFC Naples.

**Q:** Does the existing doctrine allows for the understanding of InfoOps contribution to Information Superiority?

**KOR:** You defined information superiority as "the operational advantage that comes from the capability to collect, processes and disseminate a constant flow of information, while exploring or denying the capability of an adversary to do the same". I do think, that INFOOPS supports the effort to increase information superiority, but it is not the main effort. INFOOPS focuses more on communication than on information, which describes a monologue between sender and recipient. In the 21st century and after the digital revolution the term "information superiority" should be revised and re-defined completely. I do think that it is no longer achievable. Per definition InfoOps is "a staff function to analyse, plan, assess and integrate information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and NAC approved audiences in support of Alliance mission objectives. (…) As a staff function InfoOps provides the COM with an assessment of the Information Environment (IE) and a mechanism to plan and coordinate Information Activities (IA) on a continuous basis to achieve effects in support of operational objectives. (…) NATO StratCom guidance enables the synchronisation of all information and communication activities. NATO InfoOps supports StratCom by planning to achieve effects and coordinating IA on the operational and tactical levels in accordance with the COM's operational objectives." Information activities are actions designed to affect information or information systems. They can be performed by any actor and include protection measures. Information effects are desired conditions created in the information environment as a result of information activities (must be measurable to enable analysis, planning, execution and assessment). As you can see, the context is a little bit different.

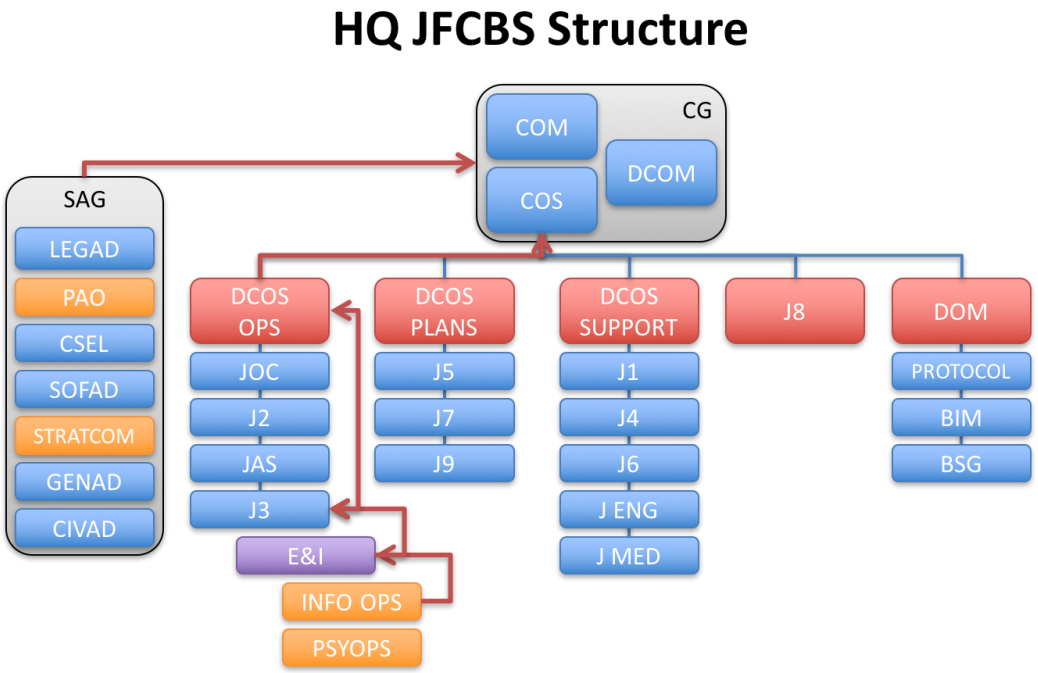
## 2. Organization

**Q:** Is there a dedicated InfoOps planning element in your organization?

**KOR:** Yes. Within the InfoOps section three peacetime establishment (PE) post are dedicated to planning.

**Q:** How does it fit within the organization?

**KOR:** InfoOps as a section (head: OF-5) is part of the Effects and Influence branch (head: OF-5), which is part of J3 division (head: OF-6) and the Operations directorate (head: OF-7). The InfoOps planners are fully integrated in the overall HQ planning process and decision making process.




**Q:** How is it organized (# Personnel/Sections, etc.)?

| | |
|---|---|
| Branch Head Effects & Influence – OF 5 | |
| Section Head InfoOps – OF 5 | Section Head PsyOps– OF 5 |
| SO InfoOps Plans – OF 4 | SO PsyOps Targeting – OF 4 |
| SO InfoOps Plans – OF 4 | SO PsyOps Training Support – OF 4 |
| SO InfoOps Plans – OF 4 | SO PsyOps Campaign Assessment – OF 4 |
| SO InfoOps Synchronisation – OF 4 | SO PsyOps Operational Assessment – OF 4 |
| SO InfoOps Synchronisation – OF 4 | SO PsyOps Future Plans – OF 4 |
| SO InfoOps Targeting– OF 4 | SO PsyOps Current Plans – OF 4 |
| SO InfoOps Targeting– OF 4 | SO PsyOps Crisis Response Planning – OF 4 |
| SO InfoOps Key Leader Engagement – OF 4 | SO PsyOps Current Ops – OF 4 |
| SO InfoOps Strategic Engagements – OF 4 | SO PsyOps Target Audience Analysis – OF 4 |
| SO InfoOps Situational Awareness – OF 3 | Staff Assistant – OR 6 |
| SO InfoOps Counter IED – OF 4 | |
| SO InfoOps Assessment – OF 4 | |
| SO InfoOps Assessment – OF 3 | |
| SO InfoOps Assessment – OF 4 | |
| SO InfoOps LI/LL– OF 4 | |
| Staff Assistant – OR 6 | |

## 3. Training

**Q:** Is InfoOps planning included in the regular training activities for your organization?

**KOR:** Yes, InfoOps is fully integrated in all activities.

**Q:** Does the training allow for the understanding on how InfoOps contributes to Information Superiority?

**KOR:** Yes, it does, with the difficulties I mentioned above.

**4. Material**

**Q:** Does the Software Planning / Execution Tools (TOPFAS or other) allow for the planning, coordination and integration of the different Capabilities and Techniques integrated by InfoOps in support of the mission?

**KOR:** Yes, TOPFAS is an adequate tool, if used properly. Unfortunately, this is not always the case. Actually, coordination, synchronisation and integration is not very much dependent on a tool, it more a process between individual actors conducted during working groups and coordination boards (battle rhythm).

**5. Leadership**

**Q:** Does the Staff have the adequate training to plan InfoOps? What training is mandatory and/or advisable?

**KOR:** Yes, the training opportunities are adequate. There are several national training opportunities, within the NATO community Italy took the lead for that (courses in English language are offered i.e. by ITA, CAN, DEU, USA, etc.). In addition, NATO School Oberammergau (NSO) offers several courses related to the different levels of communication disciplines, i.e.

- InfoOps Planners Course
- PSYOPS Planners Course
- Senior InfoOps (Introduction) Course
- StratCom Course
- StratCom Practitioners Course
- Etc.

The InfoOps planners course is mandatory for all JFCBS InfoOps personnel.

**Q:** Does the Leadership integrate InfoOps in the Operational planning?

**KOR:** Yes, fully.

Does the Leadership promote information sharing between the different staff elements?

**KOR:** Yes, it does, but this has nothing to do with InfoOps. The name is misleading, as I pointed out above.

**Q:** Does the Leadership promote information sharing with the Component Commands and with external entities (IAW NATO Information Assurance regulations)?

**KOR:** Yes, it does, but this has nothing to do with InfoOps. The name is misleading, as I pointed out above.

**6. Personnel**

**Q:** Does the InfoOps planning element in your organization has a PE manning?

**KOR:** Yes, stated above.

**Q:** How does it differ from PE to CE?

**KOR:** No difference when it comes to planning.

**Q:** During an Exercise / CRO where does the augmentee staff elements come from?

**KOR:** The augmentees come from NATO Command Structure (NCS), NATO Force Structure (NFS) or from national HQs.

**7. Interoperability**

**Q:** The above-mentioned Software tools allow information sharing?

**KOR:** Yes, TOPFAS provides a collaborative working environment.

**Q:** The network allows for the integration of Sensors, Information and Combat Platforms?

**KOR:** Yes, in general.

**8. Information Superiority**

**Q:** In your perspective, how does the InfoOps planning, coordinating and synchronization cell contribute to the JFC Information Superiority?

**KOR:** As already described, I do not think information superiority can be achieved in modern times. Yes, InfoOps analysis and assessment does contribute to the overall picture and supports the effort to increase the understanding of a conflict. InfoOps is just a staff function, not a capability and InfoOps does not conduct operations in the information domain. By defining information effects and coordinating information activities within the overall campaign, InfoOps does support the overall StratCom effort in support of the operational effects.