

NÃO CLASSIFICADO



MINISTÉRIO DA DEFESA NACIONAL
EXÉRCITO PORTUGUÊS

PDE 2-00

INFORMAÇÕES, CONTRA-INFORMAÇÃO E SEGURANÇA

Março de 2009

NÃO CLASSIFICADO

NÃO CLASSIFICADO



MINISTÉRIO DA DEFESA NACIONAL
EXÉRCITO PORTUGUÊS

PDE 2-00

INFORMAÇÕES, CONTRA-INFORMAÇÃO E SEGURANÇA

Março de 2009

NÃO CLASSIFICADO

Página intencionalmente em branco

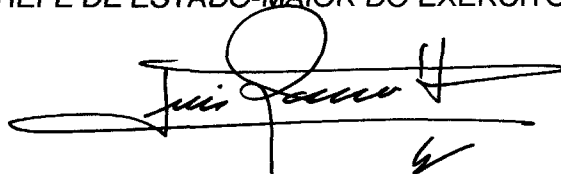
NÃO CLASSIFICADO

DESPACHO

1. Aprovo, para utilização no Exército, a PDE 2-00 Informações, Contra-Informação e Segurança.
2. A PDE 2-00 é uma publicação não classificada.
3. É permitido copiar ou fazer extractos desta publicação, sem autorização da entidade promulgadora.
4. A PDE 2-00 entra imediatamente em vigor e substitui o Regulamento de Campanha - Informações, de 7 de Agosto de 2007.
5. A presente versão está de acordo com a PAD 320-01 Publicações do Exército em vigor aprovada em 19 de Dezembro de 2008.

Lisboa, 14 de Abril de 2007

O CHEFE DE ESTADO-MAIOR DO EXÉRCITO

A handwritten signature in black ink, appearing to read 'José Luís Pinto Ramalho', is written over a horizontal line. There is a small mark to the right of the signature.

JOSÉ LUÍS PINTO RAMALHO

GENERAL

NÃO CLASSIFICADO

Página intencionalmente em branco

REGISTO DE ALTERAÇÕES

IDENTIFICAÇÃO DA ALTERAÇÃO (Nº e Data)	DATA DA INTRODUÇÃO	ENTRADA EM VIGOR (Data)	IDENTIFICAÇÃO DE QUEM INTRODUZIU (Ass, Posto, Unidade)

Página intencionalmente em branco

ÍNDICE

1ª PARTE
INFORMAÇÕES

CAPÍTULO 1 AS INFORMAÇÕES NO AMBIENTE OPERACIONAL 1-1

SECÇÃO I – O AMBIENTE OPERACIONAL, PAPEL E PRINCÍPIOS
DAS INFORMAÇÕES

0101. O Ambiente Operacional	1-1
0102. O Papel das Informações	1-2
0103. Princípios das Informações	1-3

SECÇÃO II – DADOS, NOTÍCIAS E INFORMAÇÕES

0104. Dados	1-4
0105. Notícias	1-4
0106. Informações	1-5

SECÇÃO III – NÍVEIS E TIPOS DE INFORMAÇÕES

0107. Níveis das Informações	1-6
0108. Tipos das Informações	1-7

CAPÍTULO 2 DISCIPLINAS E ÁREAS FUNCIONAIS DAS INFORMAÇÕES 2-1

SECÇÃO I – INTRODUÇÃO

0201. Generalidades	2-1
0202. Origens	2-1
0203. Órgãos	2-1

SECÇÃO II – DISCIPLINAS DAS INFORMAÇÕES

0204. Generalidades	2-2
0205. Informação Humana	2-2
0206. Informação de Imagens	2-3
0207. Informação de Transmissões Electromagnéticas e Comunicações	2-6
0208. Informação de Medição e Assinatura Electromagnética	2-6

PDE 2-00 Informações, Contra-Informação e Segurança

SECÇÃO III – ÁREAS FUNCIONAIS DAS INFORMAÇÕES

0209. Generalidades	2-8
0210. Informações Biográficas	2-8
0211. Informações Económicas	2-8
0212. Informações de Engenharia	2-9
0213. Informações sobre Forças Armadas	2-9
0214. Informações Geoespaciais	2-9
0215. Informações sobre Infra-Estruturas	2-9
0216. Informações Logísticas	2-9
0217. Informações Médicas	2-9
0218. Informações Políticas	2-9
0219. Informações de Segurança	2-10
0220. Informações Sociológicas	2-10
0221. Informações sobre Targeting	2-10
0222. Informações Técnicas e Científicas	2-10
0223. Informações Técnicas	2-10

CAPÍTULO 3 O CICLO DA PRODUÇÃO DA INFORMAÇÃO 3-1

SECÇÃO I – GENERALIDADES

0301. O Ciclo da Produção da Informação	3-1
0302. Definições	3-2

SECÇÃO II – ORIENTAÇÃO DO ESFORÇO DE PESQUISA

0303. Definição	3-3
0304. Necessidades de Informação Crítica do Comandante	3-4
0305. Necessidades Prioritárias de Informações	3-5
0306. Necessidades de Informação sobre Forças Amigas	3-5
0307. Elementos Essenciais de Informação das Forças Amigas	3-5
0308. Necessidades de Informação	3-6
0309. Indicadores	3-6
0310. Conceito de Gestão das Necessidades de Informação e Coordenação da Pesquisa	3-7

SECÇÃO III – PESQUISA

0311. Introdução	3-8
0312. Princípios da Pesquisa	3-9

0313. A Exploração de Origens e Órgãos	3-10
0314. Tipos de Origens e Órgãos	3-10
0315. Selecção de Origens e Órgãos	3-11
0316. Entrega da Informação	3-12
0317. A Natureza do Plano de Pesquisa	3-13

SECÇÃO IV – PROCESSAMENTO

0318. Introdução	3-13
0319. Registo	3-14
0320. Factores que Afectam o Registo	3-15
0321. Avaliação	3-16
0322. Análise e Integração	3-18
0323. Abordagem Multidisciplinar	3-18
0324. Interpretação	3-18
0325. O Produto Final	3-19
0326. O Processo Mental	3-19
0327. Maximização do Uso da Informação	3-19
0328. Decepção	3-20
0329. Confirmação	3-20
0330. Considerações Finais	3-20

SECÇÃO V – DISSEMINAÇÃO

0331. Definição	3-20
0332. Princípios da Disseminação	3-21
0333. Formatos da Disseminação	3-23
0334. Princípios da Disseminação Verbal	3-23
0335. Tipos de Exposições Verbais	3-24
0336. Canais de Comunicação	3-24
0337. As Vantagens e Inconvenientes da Exposição Verbal	3-24
0338. Princípios da Disseminação Escrita	3-25
0339. Documentos de Disseminação	3-25
0340. Disseminação Electrónica de Dados	3-29
0341. Comunicações	3-30

CAPÍTULO 4 PROCEDIMENTOS 4-1

**SECÇÃO I – GESTÃO DA COORDENAÇÃO DA PESQUISA
E DAS NECESSIDADES DE INFORMAÇÕES**

0401. Metodologia	4-1
0402. Gestão da Pesquisa	4-1
0403. Gestão das Necessidades de Informações	4-2
0404. Coordenação da Pesquisa	4-3
0405. Procedimentos da Secção de CCIRM	4-4

SECÇÃO II – OPERAÇÕES DE INFORMAÇÃO

0406. Generalidades	4-5
0407. O Ambiente da Informação	4-5
0408. A Conduta das Operações de Informação	4-6
0409. Princípios de Operações de Informação	4-6
0410. Apoio das Informações às INFO OPS	4-8

SECÇÃO III – PROCESSO DE PLANEAMENTO OPERACIONAL

0411. Processo de Planeamento Operacional	4-8
---	-----

**SECÇÃO IV – ESTUDO CONJUNTO DO ESPAÇO DE BATALHA
PELAS INFORMAÇÕES**

0412. Generalidades	4-12
0413. Uso do Estudo Conjunto do Espaço de Batalha pelas Informações	4-13
0414. Conceito de Estudo Conjunto do Espaço de Batalha pelas Informações	4-13
0415. Processo do Estudo Conjunto do Espaço de Batalha pelas Informações e o Ciclo da Produção da Informação	4-14
0416. Processo de Estudo Conjunto do Espaço de Batalha pelas Informações	4-14
0417. Aplicação	4-18
0418. Estudo Conjunto do Espaço de Batalha pelas Informações e o Processo de Targeting	4-18

**SECÇÃO V – INFORMAÇÕES, VIGILÂNCIA, AQUISIÇÃO DE OBJECTIVOS E
RECONHECIMENTO CONJUNTO**

0419. Fundamentos	4-19
0420. Elementos	4-19
0421. Actividades	4-20
0422. Princípios e Considerações	4-21

0423. Apoio ao Planeamento Operacional	4-23
0424. A Imagem Operacional Comum	4-23
0425. Apoio ao Targeting	4-24
0426. Apoio às Operações de Informações	4-25
0427. Apoio à Protecção da Força	4-25
0428. Operações Multinacionais	4-25
0429. Planeamento	4-26
0430. Produtos de Planeamento ISTAR	4-27
0431. Plano de Pesquisa	4-27
0432. Apêndice ISTAR	4-28
0433. Matriz de Sincronização ISTAR	4-28
0434. Aperfeiçoamento do Plano	4-28
0435. Parâmetros de Planeamento	4-28
0436. Planeamento de Atribuição de Meios	4-29
0437. Planeamento do Emprego dos Meios	4-30
0438. Comando e Controlo	4-30
0439. Funções de Comando e Controlo	4-31
0440. A Função de Coordenação de ISTAR	4-32
0441. A Função de Pesquisa	4-32
0442. ISTAR e o Processo de Targeting	4-32
0443. A Arquitectura ISTAR da OTAN	4-33
0444. Contribuições Nacionais para a Arquitectura ISTAR OTAN	4-37

SECÇÃO VI – PROCESSO DE TARGETING

0445. Generalidades	4-38
0446. O Processo	4-38
0447. Objectivos	4-38
0448. O Ciclo do Targeting	4-39
0449. Passos	4-41
0450. Terminologia de Targeting	4-41
0451. Os Princípios Legais de Targeting	4-43
0452. Apoio das Informações ao Targeting	4-44
0453. Conclusão	4-45

SECÇÃO VII – O ESTUDO DA SITUAÇÃO DE INFORMAÇÕES

0454. Objectivo	4-45
0455. Metodologia	4-46
0456. Factores a Considerar	4-46

PDE 2-00 Informações, Contra-Inteligência e Segurança

0457. Princípios	4-47
0458. Orientação Adicional	4-47
0459. O Estudo da Situação de Informações e o Estudo Conjunto do Espaço de Batalha pelas Informações	4-48

SECÇÃO VIII – O APOIO DAS INFORMAÇÕES A OPERAÇÕES DE
CONTRA-TERRORISMO

0460. Generalidades	4-49
0461. Restrições Nacionais	4-50
0462. A Natureza da Informação de Contra-Terrorismo	4-50
0463. Origens de Contra-Terrorismo	4-52
0464. Bases de Dados de Informações e Software	4-53
0465. Estudo Conjunto do Espaço de Batalha pelas Informações	4-53
0466. Informações, Vigilância, Aquisição de Objectivos e Reconhecimento	4-54
0467. Targeting	4-55

SECÇÃO IX – AS INFORMAÇÕES NAS OPERAÇÕES DE RESPOSTA A CRISES

0468. Introdução	4-55
0469. Informações, Vigilância, Aquisição de Objectivos e Reconhecimento	4-55
0470. Informação Humana	4-56
0471. Necessidades de Informações	4-56
0472. Indicadores	4-56
0473. Planeamento	4-57

CAPÍTULO 5 ARQUITECTURA DO SISTEMA DAS INFORMAÇÕES 5-1

SECÇÃO I – A ARQUITECTURA DAS INFORMAÇÕES NA OTAN

0501. Generalidades	5-1
0502. Princípios	5-1
0503. Capacidade de Comunicações	5-3
0504. Planeamento da Arquitectura	5-3

SECÇÃO II – CONTRIBUIÇÕES NACIONAIS E MULTIPLOS DOMINIOS

0505. Generalidades	5-5
0506. Finalidade	5-6
0507. Funcionalidade	5-6
0508. Grupos Principais de Informações	5-6
0509. Comunicações	5-8

0510. A Responsabilidade das Células de Informações	5-9
---	-----

SECÇÃO III – O APOIO DOS SISTEMAS DE INFORMAÇÃO GEOGRÁFICA ÀS INFORMAÇÕES

0511. Os Sistemas de Informação Geográfica	5-9
0512. Os Dados Geoespaciais	5-10

SECÇÃO IV – BASES DE DADOS DAS INFORMAÇÕES

0513. Formatos	5-11
0514. Bases de Dados Relacionais	5-11
0515. Bases de dados Normalizadas	5-12
0516. A Gestão de Bases de Dados	5-12

CAPÍTULO 6 NÍVEL OPERACIONAL DAS OPERAÇÕES 6-1

SECÇÃO I – INTRODUÇÃO

0601. Generalidades	6-1
0602. Operações Conjuntas	6-1
0603. Informações Conjuntas	6-2

SECÇÃO II – NATUREZA DAS INFORMAÇÕES NO NÍVEL OPERACIONAL

0604. Papel das Informações	6-3
0605. Finalidade das Informações no Nível Operacional	6-3
0606. Perspectiva Geral das Necessidades de Informações	6-5
0607. Inimigo	6-5
0608. Ambiente Operacional	6-6

SECÇÃO III – O APOIO DAS INFORMAÇÕES AO PLANEAMENTO

0609. Generalidades	6-8
0610. Processo de Planeamento Operacional	6-8
0611. Estudo Conjunto do Espaço de Batalha pelas Informações	6-11

SECÇÃO IV – O APOIO DAS INFORMAÇÕES ÀS OPERAÇÕES

0612. Generalidades	6-11
0613. Informações, Vigilância, Aquisição de Objectivos e Reconhecimento	6-11
0614. O Processo de Targeting Conjunto	6-12
0615. O Ciclo de Targeting	6-13
0616. Targeting e o Plano de Campanha	6-13

PDE 2-00 Informações, Contra-Inteligência e Segurança

0617. Targeting Conjunto – Resumo	6-14
0618. As Informações e Operações de Informação no nível Operacional	6-14
0619. As Informações no apoio às Operações Pós-Conflito	6-15

SECÇÃO V – ARQUITECTURA CONJUNTA DAS INFORMAÇÕES

0620. Objectivo	6-15
0621. Características	6-16
0622. Considerações sobre o Planeamento	6-16
0623. Necessidades	6-17
0624. Quartel-General da Força Tarefa Conjunta Combinada	6-18
0625. Apoio das Informações	6-19
0626. Condições	6-20
0627. Princípios	6-20
0628. Centro de Informações Conjunto	6-20
0629. Células Nacionais de Informações	6-21

CAPÍTULO 7 NÍVEL TÁCTICO DAS OPERAÇÕES 7-1

SECÇÃO I – GENERALIDADES

0701. Introdução	7-1
0702. Nível Tático	7-1
0703. O Papel das Informações ao Nível Tático	7-2
0704. A Importância das Informações ao Nível Tático	7-2
0705. Dimensões	7-2
0706. O Papel do Estado-Maior	7-3

SECÇÃO II – AS INFORMAÇÕES E O PROCESSO DE DECISÃO MILITAR

0707. Generalidades	7-4
0708. As Responsabilidades e Tarefas do Oficial de Informações durante o PDM	7-6

SECÇÃO III – *TARGETING*

0709. Generalidades	7-8
0710. Função Decidir	7-9
0711. Designação de Objectivos	7-10
0712. Produtos da Função Decidir	7-11
0713. Definição de Objectivos	7-13
0714. Função Detectar	7-14

0715. Função Seguir	7-14
0716. Relatórios	7-15
0717. Função Atribuir	7-15
0718. Função Avaliar	7-16

SECÇÃO IV – O CICLO DA PRODUÇÃO DA INFORMAÇÃO

0719. Passos	7-17
0720. Finalidade do Ciclo da Produção da Informação	7-18
0721. Orientação do Esforço de Pesquisa	7-18
0722. Pesquisa	7-19
0723. Bases de Dados das Informações	7-21
0724. Processamento	7-21
0725. Registo	7-21
0726. Ferramentas de Registo	7-22
0727. Disseminação	7-22
0728. ISTAR ao Nível Tático	7-22
0729. Planeamento ISTAR	7-22

2ª PARTE

CONTRA-INFORMAÇÃO E SEGURANÇA

CAPÍTULO 8 INTRODUÇÃO	8-1
------------------------------------	------------

SECÇÃO I – CONCEITOS

0801. Conceitos	8-1
-----------------------	-----

SECÇÃO II – A AMEAÇA À SEGURANÇA

0802. Actividades de Segurança	8-2
--------------------------------------	-----

SECÇÃO III – TIPOS DE AMEAÇA

0803. Espionagem	8-4
0804. Sabotagem	8-6
0805. Subversão	8-6
0806. Terrorismo	8-7
0807. Crime Organizado	8-8

PDE 2-00 Informações, Contra-Informação e Segurança

SECÇÃO IV – NEUTRALIZAÇÃO DA AMEAÇA

0808. Responsabilidade pela Neutralização da Ameaça	8-8
---	-----

SECÇÃO V – PRINCIPIOS ORIENTADORES DA CI E DAS OPERAÇÕES
DE SEGURANÇA

0809. Princípios	8-10
------------------------	------

CAPÍTULO 9 CONTRA-INFORMAÇÃO 9-1

SECÇÃO I – O PAPEL DA CONTRA-INFORMAÇÃO

0901. O Papel da Contra-Informação	9-1
--	-----

SECÇÃO II – NORMAS DA CONTRA-INFORMAÇÃO

0902. Introdução	9-2
0903. A Contra-Informação em Operações Multinacionais	9-2

SECÇÃO III – PROCESSO DE CONTRA-INFORMAÇÃO

0904. Processo da Contra-Informação	9-3
0905. Estudo de Contra-Informação	9-3
0906. Planeamento de Contra-Informação	9-4
0907. Pesquisa de Contra-Informação	9-4
0908. Avaliação da Ameaça	9-5
0909. Contra-Medidas de Contra-Informação	9-6

SECÇÃO IV – AS NECESSIDADES DE CONTRA-INFORMAÇÃO

0910. Necessidades de Contra-Informação	9-7
---	-----

CAPÍTULO 10 SEGURANÇA NAS OPERAÇÕES 10-1

SECÇÃO I – AVALIAÇÃO DA AMEAÇA

1001. Generalidades	10-1
---------------------------	------

SECÇÃO II – MEDIDAS DE PROTECÇÃO

1002. Definição	10-1
1003. Medidas de Segurança do Pessoal	10-2
1004. Medidas de Segurança Física	10-2
1005. Medidas de Segurança Organizacional	10-3

1006. Medidas de Segurança da Informação e Processamento Automático de Dados	10-5
SECÇÃO III – NEUTRALIZAÇÃO DA AMEAÇA	
1007. Responsabilidade	10-5
SECÇÃO IV – PROTECÇÃO DA FORÇA	
1008. Generalidades	10-6
1009. Objectivos da Protecção da Força	10-7
SECÇÃO V – COMPONENTES DA PROTECÇÃO DA FORÇA	
1010. Introdução	10-7
1011. Segurança das Operações	10-8
1012. Contra-Vigilância	10-9
1013. Decepção	10-9
1014. Ligação da Contra-Vigilância, da Segurança das Operações e da Decepção	10-10
1015. Medidas de Protecção	10-10
1016. Segurança no Terreno	10-11
1017. Passagem de Informação	10-12
1018. Papel da Contra-Informação e Segurança	10-13
1019. Fluxo da Informação Adequada	10-13
SECÇÃO VI – DISSEMINAÇÃO DA CONTRA-INFORMAÇÃO E SEGURANÇA	
1020. Generalidades	10-14
1021. Relatórios	10-15
1022. Princípios da Disseminação da Contra-Informação e da Segurança	10-16
ANEXO A – PLANO DE PESQUISA	A-1
ANEXO B – ESTUDO DA SITUAÇÃO DE INFORMAÇÕES	B-1
ANEXO C – ANEXO DE INFORMAÇÕES	C-1
GLOSSÁRIO DE TERMOS E DEFINIÇÕES	1
GLOSSÁRIO DE ABREVIATURAS	1

Página intencionalmente em branco

Nota Prévia

A Publicação PDE 2-00 INFORMAÇÕES, CONTRA-INFORMAÇÃO E SEGURANÇA, que se apresenta para promulgação pretende estabelecer a base conceptual da Doutrina do Exército Português para as áreas das Informações, da Contra-informação e da Segurança. Tem como principais referências as Allied Joint Publication 2.0, 2.1 (A) e 2.2, da OTAN, bem como os FM 2-0 e FM 34-130 do Exército dos EUA.

Em relação às publicações anteriormente referidas foram introduzidas diversas alterações que se justificam pela:

- Vantagem em manter terminologia tradicionalmente utilizada pelo Exército Português, nos casos em que o significado dos termos, definições ou expressões utilizados não diferissem substancialmente;
- Dificuldade em traduzir para português algumas expressões técnicas, não directamente relacionadas com a doutrina e terminologia de Informações;
- Interesse em salientar procedimentos ainda não adoptados no Exército Português.

A Publicação encontra-se estruturada em Parte I – INFORMAÇÕES e Parte II – CONTRA-INFORMAÇÃO E SEGURANÇA, abordando cada uma delas os assuntos respectivos. Constitui a principal referência para o Exército Português no âmbito do planeamento e conduta das Informações em todo o espectro dos conflitos.

A Publicação PDE 2-00 INFORMAÇÕES, CONTRA-INFORMAÇÃO E SEGURANÇA resulta da adaptação do Regulamento de Campanha Informações, aprovado pelo Despacho do Exmo GEN CEME de 07AGO07, às normas estabelecidas para as PDE pela “PAD 320-01 Publicações do Exército” aprovada por despacho do Exmo GEN CEME de 19DEC08 e por conseguinte revoga o referido regulamento.

As alterações e comentários que possam melhorar a compreensão e objectividade deste documento devem ser endereçados à Direcção de Doutrina.

O DIRECTOR DE DOCTRINA



ANÍBAL ALVES FLAMBÓ

MAJOR-GENERAL

Página intencionalmente em branco

1ª PARTE

INFORMAÇÕES

CAPÍTULO 1 AS INFORMAÇÕES NO AMBIENTE OPERACIONAL

SECÇÃO I – O AMBIENTE OPERACIONAL, PAPEL E PRINCÍPIOS DAS INFORMAÇÕES

0101. O Ambiente Operacional

A situação do mundo é complexa e influenciada por actores diversos e um grande número de possibilidades de conflitos, o que obriga a que as forças militares enfrentem um ambiente operacional global, dinâmico, multidimensional e cada vez mais interligado. Além disso, a contínua mudança das características da guerra, consequência das constantes alterações da natureza dos conflitos, obriga à permanente adaptação das operações de informações às diferentes ameaças, área de operações e ambiente operacional em mudança. Isto obriga a que todo o pessoal ligado às informações mantenha ou adquira muito rapidamente o conhecimento cultural (a um elevado nível de detalhe) específico para o ambiente regional e local na área de operações. Estas circunstâncias afectam significativamente as informações, uma vez que aumentam o grau de dificuldade e de complexidade em determinar não somente quem constitui o inimigo¹, mas também qual das possíveis modalidades de acção este poderá levar a cabo.

Se pudermos dominar um inimigo pela diferença de potencial militar ou potencialidades tecnológicas, organizacionais e estratégicas, o inimigo recorrerá a modos e meios menos convencionais e adaptáveis para conseguir os seus fins, os quais podem mudar. O pessoal ligado às informações deve também adaptar as suas operações e modo de pensar de forma a compreender e antecipar a acção do inimigo. Deve preservar um espírito vigilante, já que todo o possível inimigo é uma ameaça adaptável, dotada de extensos recursos criados e mantidos através da aquisição de capacidades específicas e do apoio dos aliados.

Por exemplo, o inimigo pode:

- usar táticas destinadas a infligir um grande número de baixas militares ou civis ou atacar pessoas de elevado estatuto;

¹ Inimigo, adversário ou oponente de acordo com a situação. Consultar o glossário.

PDE 2-00 Informações, Contra-Informação e Segurança

- atingir e destruir subsistemas de um sistema operativo, individualmente ou colectivamente;
- usar a população civil local como cobertura e sustentação;
- usar as características do ambiente natural, industrial e empresarial contra as nossas forças nos modos mais diversos;
- estudar cada aspecto da nossa doutrina, treino e potencialidades tecnológicas;
- superar rapidamente todas as contramedidas postas em prática pelas nossas forças para anular as suas actividades;
- empregar pessoal para conduzir acções de reconhecimento, assim como população civil local que apoie a ameaça;
- atacar as nossas informações, sistemas de informação e infra-estruturas de decisão, a fim de desacreditar ou provocar, enfraquecer alianças e coligações, degradar o apoio da opinião pública, incitar à condenação interna e internacional, e degradar os nossos sistemas de comando e controlo e/ou potencialidades do sistema Informações, Vigilância, Aquisição de Objectivos e Reconhecimento (ISTAR - Intelligence, Surveillance, Target Acquisition and Reconnaissance).

A capacidade de derrotar tais inimigos depende, em grande medida, da habilidade do pessoal ligado às informações em analisar os actuais e futuros métodos e as capacidades dos potenciais inimigos, bem como de incorporar aquelas considerações no seu treino, planeamento e execução de operações militares. O ambiente operacional continuará a mudar, pelo que as nossas forças armadas e informações militares devem continuar a evoluir para manter a capacidade de fornecer informações.

0102. O Papel das Informações

As informações são uma responsabilidade do comando. O comandante deve dirigir o processo das informações e, apesar de ter uma célula de informações para o aconselhar, deve ter uma clara compreensão do processo das informações, das suas capacidades e limitações. Deve conseguir definir, de forma sucinta, as suas necessidades de informações e interpretar as informações recebidas em resposta às necessidades e de acordo com a sua missão.

As informações fornecem ao comandante uma avaliação das modalidades de acção, capacidades, potencial de combate, dispositivo e organização do inimigo, bem como uma previsão das suas intenções. Fornecem, também, uma avaliação da influência das características da área de operações no cumprimento da nossa missão e na do inimigo,

assim como uma avaliação das nossas acções sobre o inimigo. A posse de informações permite que o comandante possua uma vantagem importante sobre o seu inimigo, prevendo as acções e reacções que ele possa adoptar. Assim o comandante pode planear as suas operações com base no conhecimento do inimigo, diminuindo o risco tático e aumentando as suas possibilidades de obtenção de sucesso na condução das operações.

As informações nunca estarão completas e haverá sempre algumas perguntas sem resposta quando se tenta caracterizar um inimigo. As informações nunca podem ser consideradas certas absolutas, mas apenas estimativas, que consoante a sua precisão têm maior ou menor peso na decisão do comandante.

0103. Princípios das Informações

Existem oito princípios básicos que norteiam a produção de informações e a organização e actividades daqueles que conduzem o processo de informações. São os seguintes:

- **Controlo Centralizado.** As informações devem ser controladas de forma centralizada, para evitar a duplicação de trabalho não autorizado, fornecer o apoio mútuo e assegurar o uso eficiente e económico de todos os recursos;
- **Oportunidade.** As informações são inúteis se chegarem ao seu destino demasiado tarde. Pela mesma razão, o sistema através do qual são atribuídas as ordens de pesquisa às origens e órgãos, deve ser capaz de reflectir, sem atraso, quaisquer alterações significativas nas necessidades ou prioridades de informações;
- **Exploração Sistemática.** As origens e órgãos devem ser explorados de forma sistemática e metódica, com base no conhecimento das suas capacidades e limitações;
- **Objectividade.** Deve-se resistir a toda a tentativa de distorcer a informação para servir ideias pré-concebidas;
- **Acessibilidade.** As notícias e as informações relevantes devem ser imediatamente disponibilizadas às células de informações e aos utilizadores. Todas as notícias e informações devem ser processadas pelas células de informações, que as compara com os dados obtidos antecipadamente. As informações não têm nenhum valor se não forem disseminadas ou não estiverem acessíveis àqueles que delas necessitam;
- **Capacidade de Resposta.** A célula de informações deve antecipar-se e ter capacidade de resposta às necessidades de informações do comandante, em todos os momentos;

PDE 2-00 Informações, Contra-Informação e Segurança

- **Protecção da Fonte.** Todas as fontes de informação devem ser protegidas adequadamente;
- **Revisão Contínua.** As informações devem ser continuamente revistas onde se torne necessário, tendo em consideração toda a informação nova e comparando-a com a já existente.

SECÇÃO II – DADOS, NOTÍCIAS E INFORMAÇÕES

0104. Dados

Os dados incluem sinais detectados por um sensor, ou origem de qualquer tipo (humano, mecânico ou electrónico), ou transmitidos entre quaisquer pontos nodais de um sistema. Pode haver a necessidade de serem trabalhados (alteração do seu formato) de forma a serem perceptíveis e lhes ser atribuído um significado.

0105. Notícias

Entende-se por notícia todo o dado não processado de qualquer natureza (facto, documento ou material) que pode ser usado na produção de informações. É um comunicado sobre o estado da situação que existe, ou que existiu, num determinado momento ou espaço. É de natureza indiscutível e pode estar relacionada com acontecimentos do passado ou do presente, sendo histórico ou actual.

Em operações, o comandante terá acesso a grandes quantidades de notícias relativas a todos os aspectos do ambiente operacional. A notícia estar-lhe-á disponível e irá cobrir um vasto leque de assuntos relativos à identidade, equipamento, localização, situação dos reabastecimentos, situação em baixas, estado dos reforços, situação em combustíveis e munições e, ainda, outros aspectos relativos quer à sua força quer à do inimigo. Haverá também um grande volume de notícias relativas ao ambiente do espaço de batalha, ao clima, ao tempo, ao terreno, às influências sócio-políticas e outros aspectos do espaço de batalha.

Na preparação para levar a cabo o processo de tomada de decisão, o comandante será capaz de identificar, à partida, que informação quer sobre o inimigo ou sobre as forças amigas e que vai necessitar a fim de poder chegar a uma decisão e elaborar o seu plano.

As questões às quais ele precisa de responder dão origem às Necessidades de Informação Crítica do Comandante (CCIR - *Commander's Critical Information Requirements*). As CCIR compreendem as Necessidades Prioritárias de Informações

(PIR - *Priority Intelligence Requirements*) e as Necessidades de Informação sobre Forças Amigas (FFIR - *Friendly Forces Information Requirements*). As CCIR podem também incluir o Tempo de Validade da Informação (LTIOV - *Latest Time Information Of Value*) para orientar o tempo de pesquisa.

Os Elementos Essenciais de Informação das Forças Amigas (EEFI – *Essencial Elements of Friendly Information*) são prioridades do comandante sempre que ele o declare.

Estas são as questões chave de informações às quais o comandante tem de responder para o apoiarem na tomada de decisão e na elaboração do seu plano de operações.

0106. Informações

Notícia, por si só é um facto ou série de factos. Quando relacionada com outras já existentes e considerada à luz de experiências anteriores, dará origem a um novo conjunto de factos, os quais são denominados informações.

As informações divergem das notícias na medida em que, sendo resultado de um processo subjectivo de opinião, não são inequívocas e são abertas a discussão. A confrontação de mais de uma notícia entre si ou com uma base de dados e as conclusões obtidas por parte de analistas é o “processo” analítico, que está na base da produção de informações a partir da notícia.

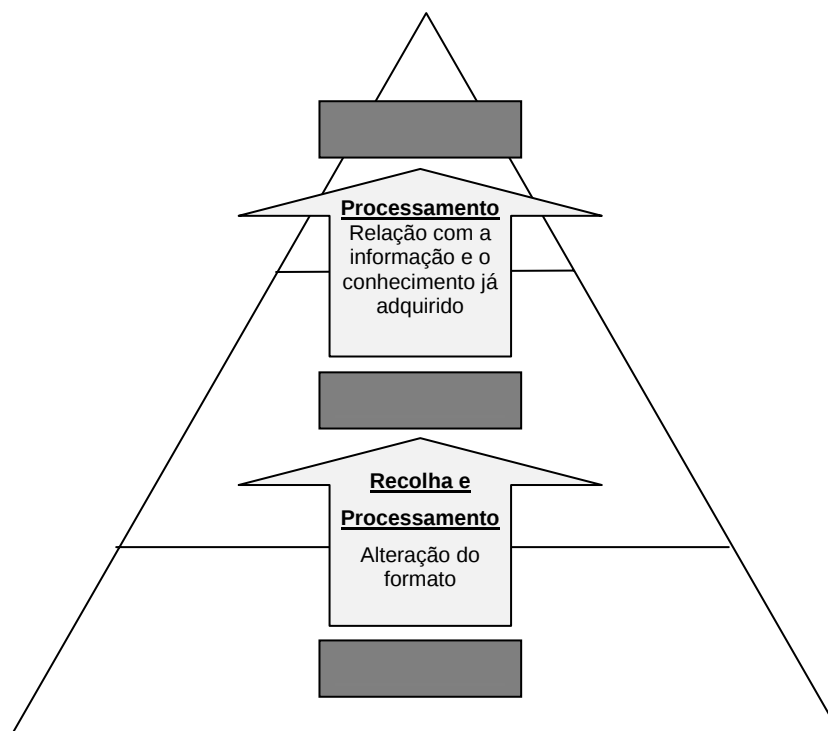


Figura 1-1 – Relação entre Notícia e Informações

PDE 2-00 Informações, Contra-Inteligência e Segurança

As informações facultam ao comandante os meios para uma previsão das prováveis táticas, possibilitando uma avaliação das capacidades do inimigo. A posse de informações dota-o de uma vantagem decisiva sobre o inimigo, sendo capaz de “entrar” na mente do inimigo e ter uma outra visão das acções ou reacção que o inimigo pode tomar. O comandante pode, deste modo, planear as suas próprias acções com base no seu conhecimento, diminuindo assim os riscos inerentes ao combate e aumentando, igualmente, a probabilidade de sucesso. Por outro lado, as informações nunca estarão completas e haverá sempre perguntas sem resposta na mente de quem está a tentar construir uma imagem do inimigo. Não existindo a garantia de que as informações são precisas, é, no entanto, possível fazer uma estimativa da sua provável precisão, o que oferece ao comandante condições para decidir que peso lhes atribuir na sua tomada de decisão.

Entende-se por informação ou informações (*intelligence*) o produto resultante do processamento de notícias respeitantes a nações estrangeiras, organizações ou elementos, reais ou potencialmente hostis, ou áreas de operações actuais ou potenciais. O termo também se aplica às actividades que visam obter o resultado final e bem assim às organizações empenhadas em tais actividades.

Entende-se, também, por informação os elementos que contribuem para o conhecimento do inimigo provável ou actual e da área de operações.

SECÇÃO III – NÍVEIS E TIPOS DE INFORMAÇÕES

0107. Níveis das Informações

Existem três níveis de informações, sendo a sua categorização baseada no uso que lhe for dada:

- **Informações Estratégicas.** Informações estratégicas são informações necessárias à formulação de planos políticos e militares, a nível nacional e internacional. Este é o mais alto nível de informações, derivado das notícias recolhidas em resposta às necessidades colocadas pelos governos nacionais, cobrindo todo o espectro de assuntos militares, diplomáticos, políticos e económicos, nacional e internacional;
- **Informações Operacionais.** Informações operacionais são informações necessárias para o planeamento e condução de campanhas ao nível operacional. Mais especificamente, são as informações necessárias ao planeamento, execução e apoio a campanhas e operações, por parte do Quartel-General Conjunto, no âmbito da Área de Operações Conjuntas (JOA – Joint Operational Area). São informações

que são produzidas no âmbito da Área de Interesse (AOI - Area of Interest) do Comandante da Força Conjunta;

- **Informações Tácticas.** Informações tácticas são as informações necessárias ao planeamento e condução de operações tácticas. São informações usadas ao nível dos quartéis-generais das unidades de baixos escalões e são produzidas nas áreas destas unidades.

0108. Tipos das Informações

Em cada nível, as informações podem ainda ser subdivididas em três tipos:

- **Informações Básicas.** Informações básicas são as informações de fundo sobre um assunto, as quais são mantidas em bases de dados e continuamente actualizadas em tempo de paz e no decurso de operações. O principal objectivo das informações básicas é a criação de um cenário logo no início das operações de forma a ir ao encontro das necessidades de informações respeitantes aos factos inalterados, tais como as características da área de operações (clima, condições meteorológicas, efemérides, terreno), as quais poderão ser levantadas em resposta às novas exigências no decurso de uma operação. São definidas como informações sobre qualquer assunto que possam servir de ponto de partida ao planeamento e à avaliação de notícias ulteriores;
- **Informações Correntes.** Informações que são produzidas em resposta às exigências de informações ligadas a operações correntes e que se referem a acontecimentos referenciados durante a operação. Definem-se por informações relativas à situação corrente, desde o nível estratégico ao táctico;
- **Informações sobre Objectivos.** Informações de objectivos definem-se por informações que retratam e localizam as componentes de um objectivo ou conjunto de objectivos e indicam as vulnerabilidades e importância relativa. As informações de objectivos fornecem indicações sobre o objectivo para o processo de *targeting*. Este processo assegura que é feita uma eficaz aplicação dos sistemas de apoio de fogos ofensivos.

Página intencionalmente em branco

CAPÍTULO 2 DISCIPLINAS E ÁREAS FUNCIONAIS DAS INFORMAÇÕES

SECÇÃO I – INTRODUÇÃO

0201. Generalidades

A notícia que depois de processada é convertida em informação é obtida por uma grande variedade de órgãos de pesquisa e recolhida em várias origens (também designadas por fontes). Assim, nos dois parágrafos que se seguem, é apresentada a distinção entre ambas.

0202. Origens

As origens de notícias são as fontes (pessoas, coisas ou acções) de que provêm todas as notícias pesquisadas acerca do inimigo e da área de operações. Uma origem pode possuir notícias adquiridas aleatoriamente, como a que pode ser obtida em resultado da audição accidental de uma qualquer conversa de café, ou pelo contrário como resultado da resposta a uma necessidade de informação, como é o caso das imagens colhidas pela câmara de vídeo de uma aeronave não-tripulada (UAV – *Unmanned Aerial Vehicle*), num voo pré-programado. A origem é assim a fonte primária da informação e/ou possui ela mesmo a informação ou, ainda, pela sua actividade revela a existência de informação. Em contraponto, um sensor será então a pessoa ou sistema que obtém a notícia para a origem. No que diz respeito ao manuseamento da notícia, a única alteração que a origem introduz é relativamente ao seu formato, por exemplo, é o que ocorre quando no contacto entre humanos se traduz de uma língua para outra, ou quando uma imagem visual é convertida para sinal digital de forma a ser transmitida num sistema de comunicações satélite, ou seja, uma origem não tem qualquer capacidade de processamento.

0203. Órgãos

Um órgão de pesquisa é qualquer indivíduo, entidade ou unidade que obtém ou processa notícias. Por oposição à origem, pode ter a capacidade de pesquisar e processar ou simplesmente a de pesquisar, necessitando neste caso de a passar a outro órgão para a processar. A designação de órgãos de pesquisa engloba igualmente os órgãos que pesquisam notícias e os órgãos que produzem informações. Assim, podem variar desde secções de reconhecimento com a missão de relatar a actividade

PDE 2-00 Informações, Contra-Informação e Segurança

inimiga, até um departamento governamental que recebe notícias de uma multiplicidade de origens e que aplica um grande esforço de processamento para as converter em informação.

SECÇÃO II – DISCIPLINAS DAS INFORMAÇÕES

0204. Generalidades

Os meios ou sistemas utilizados para observar, detectar, registar ou transmitir notícias sobre condições, situações ou acontecimentos dão origem às seguintes disciplinas das informações:

- Informação Humana (**HUMINT** - Human Intelligence);
- Informação de Imagens (**IMINT** - *Imagery Intelligence*);
- Informação de Transmissões Electromagnéticas e Comunicações (**SIGINT** - *Signals Intelligence*);
- Informação de Medição e Assinatura Electromagnética (**MASINT** - *Measurement and Signature Intelligence*).

0205. Informação Humana

HUMINT é a informação obtida de notícias fornecidas por origens humanas. É a recolha de informação, que satisfaça os requisitos de informação definidos superiormente, através da interacção entre especialistas de Informação Humana e fontes humanas presentes no Teatro de Operações. Usa a origem humana (qualquer pessoa amiga, inimiga ou neutral) como ferramenta e um leque alargado de métodos de pesquisa, ambos de forma passiva ou activa, para reunir elementos que respondam às necessidades de informação do comandante e ao cruzamento com outras origens de notícias. A HUMINT pode empregar, como órgãos de pesquisa, oficiais de informações, contra-informações e elementos de operações especiais, sendo relevante o seu papel na confirmação e/ou aumento do valor das notícias obtidas através das restantes disciplinas (IMINT, SIGINT e MASINT).

As actividades de HUMINT são as seguintes:

a. Actividade básica de HUMINT

- (1) **Ligação** – Contacto aberto com membros e organizações amigas as quais, em virtude da sua posição oficial, têm acesso a informação com potencial valor para as Informações;

- (2) **Interrogatório Táctico** - Obter informação de pessoal capturado para evitar a perda parcial ou total de informação, pela demora destes elementos a chegar a um local de interrogatório;
- (3) **Screening** – Identificar e avaliar as áreas de conhecimento ou cooperação comuns e determinar técnicas de aproximação a indivíduos que poderão ter informação de valor.

b. Operações com fontes

- (1) **Debriefing** – Interrogatório formal e sistemático de pessoal seleccionado e autorizado, por especialistas treinados, com o objectivo de reunir informação relevante. Estes incluem refugiados, desertores, civis locais e “walk-in” (indivíduos que se apresentam voluntariamente para ceder informação);
- (2) **Interrogatório** – Interrogatório sistemático e exaustivo de pessoal capturado, por pessoal de informações treinado, para obter informação com valor, enquanto mantendo as práticas previstas na Lei Internacional para os direitos humanos e dos Prisioneiros de Guerra;
- (3) **Manipulação de fontes** – Estabelecimento de uma relação com o objectivo de explorar a fonte, de uma forma sistemática e controlada, para obter informação, sem o conhecimento de outros indivíduos.

c. Operações sem fontes

- (1) **Reconhecimento móvel** – Operações conduzidas com o objectivo de responder a Necessidades de Informação (IR – *Information Requirements*) específicas, normalmente explorando fontes de pesquisa mais sensíveis;
- (2) **Vigilância Passiva Coberta** – Observação sistemática coberta de uma pessoa, local, meio ou actividade, com o objectivo de obter ou desenvolver uma informação. Pode ser conduzida por períodos de tempo mais extensos para detectar ou identificar eventos, hábitos ou padrões de comportamento.

0206. Informação de Imagens

A IMINT é a informação que tem por base imagens captadas por sensores – ópticos (do espectro visível), infravermelhos, radares e imagens multiespectrais – instalados em plataformas terrestres, navais, aéreas ou espaciais. Estes sensores produzem imagens ópticas, electrónicas, digitais, filmes, dispositivos de ecrã electrónico e outros suportes visuais. No caso da IMINT, em particular, a máxima “uma imagem vale por mil palavras” tem um relevo especial. A informação proporcionada pela imagem é clara, concisa e

PDE 2-00 Informações, Contra-Informação e Segurança

inequívoca, servindo para confirmar e complementar informações colhidas por outras origens, tendo como principal proveniência os satélites e plataformas aéreas, tripuladas e não-tripuladas.

A IMINT apoia o comandante na orientação e na preservação do seu potencial de combate, permitindo, frequentemente, esclarecer a situação no espaço de batalha.

Para além da observação humana directa, a IMINT é a única disciplina das informações que possibilita ao comandante efectuar uma observação do espaço de batalha em tempo real. Quando não existem cartas topográficas disponíveis, as imagens digitais em suporte físico ou lógico podem ser usadas em sua substituição. A IMINT pode, ainda, ser usada para actualizar mapas ou produzir sistemas de referência gráficos e detalhar determinadas missões, onde são normalmente necessários meios digitais, incluindo imagens tridimensionais, de forma a garantir um grau de resolução necessário para apoio ao seu planeamento.

a. Fontes de Imagem

Existem três grandes fontes de imagens: nacional, civil e comercial. As imagens nacionais dizem respeito àquelas que resultam da pesquisa pelos sistemas nacionais de defesa. Contudo, existem outras origens de imagens adquiridas por fontes não nacionais como as fotografias (filmes, digitais e vídeos), imagens UAV e imagens captadas através de câmaras instaladas em sistemas de armas.

(1) Nacionais

Os sistemas nacionais desenvolvem-se para apoiar especificamente as estruturas estatais e as forças militares nacionais. Este sistema responde directamente às necessidades da nação e dos comandantes das forças.

(2) Civis

Os sistemas de imagens civis são normalmente financiados pelas instituições governamentais no que respeita à sua construção, lançamento e operação. Em alguns casos os órgãos que operam estes sistemas também criam, distribuem e arquivam dados ou imagens.

(3) Comerciais

As empresas comerciais constroem, lançam e operam sistemas de imagens para obtenção de lucro. Em situações de crise, as empresas devem ser obrigadas, de acordo com as licenças estabelecidas com o governo, a disponibilizar os satélites de imagens às entidades governamentais, a custo de mercado. No entanto, as empresas não nacionais podem não ter estes acordos, o que pode fazer com que estas não disponibilizem estes meios.

b. Tipos de Sensores IMINT

Existem quatro tipos de sensores IMINT: visível (óptico), infravermelho, radar e imagem multiespectral. Cada sensor tem capacidades únicas, com vantagens e desvantagens, cabendo à célula de informações seleccionar aquele(s) que melhor cumpra(m) a missão e que proporcione(m) a melhor compreensão ao utilizador. (Ver Tabela 2.1).

SENSOR	VANTAGENS	DESVANTAGENS
Visível (Óptico) Melhor ferramenta para actividades diurnas, tempo claro e análise detalhada. Inclui vídeo e electro-ópticas.	- Fornece uma visão familiar do cenário; - Permite obter uma resolução não atingível noutros sistemas ópticos, térmicos ou radar; - Preferível para a análise detalhada e medição; - Permite visão estereoscópica.	- Restrição devido à presença de vegetação; - Limitado à luz do dia; - Reduz o tamanho da imagem.
Infravermelhos Melhor ferramenta para actividades nocturnas, tempo limpo e análise detalhada. Inclui aparelhos de infravermelhos sem imagem.	- Sensor passivo, impossível de obstruir; - Permite efectuar a filtragem; - Garante boa resolução; - Capacidade de visão nocturna.	- Não é efectivo em períodos de ausência de radiação térmica; - Produtos de interpretação difícil; - Necessidade de analistas especializados; - Não penetra nuvens.
Radar Melhor ferramenta para detectar a presença de objectos à noite e em condições de mau tempo.	- Todo o tempo; pode penetrar em neblinas, nevoeiro, nuvens e fumo; - Para uso nocturno e diurno; - Não é afectado pela luz visível ou radiação térmica; - Boa capacidade de transporte; - Larga área de cobertura; - Permite a detecção de alvos em movimento.	- Produtos de interpretação difícil; - Necessidade de analistas especializados; - Elevada assinatura electromagnética; - A vegetação e orografia condicionam o seu emprego.
Imagem Multiespectral Melhor ferramenta para efectuar o levantamento e análise do terreno.	- Grande base de dados disponível; - Combinações de banda podem ser manipuladas de forma a responder às necessidades; - As imagens podem-se juntar com outros sistemas digitais de dados para garantir mais resolução.	- Produtos de interpretação difícil; - Necessidade de analistas especializados; - Necessidade de computadores com elevada memória, capacidade de armazenamento e grande capacidade de processamento.

Tabela 2-1 – Características dos Sensores

0207. Informação de Transmissões Electromagnéticas e Comunicações

SIGINT é o termo geral para designar a Informação de Comunicações (COMINT- *Communications Intelligence*) e a Informação Electrónica (ELINT - *Electronic Intelligence*), quando não se torne necessário fazer a distinção entre os dois tipos de informação, ou para englobar os dois termos.

COMINT e ELINT são definidas por:

- **COMINT** é a informação proveniente da interceptação por outros, que não os seus destinatários previstos, de comunicações rádio e sistemas de comunicações, bem como de características técnicas dessas transmissões.
- **ELINT** é a informação proveniente da interceptação por outros, que não os seus destinatários previstos, de emissões electromagnéticas (não-comunicações, p.e. ajudas à navegação e radares), que não são comunicações rádio, bem como das suas características técnicas.

Neste contexto, o principal papel da SIGINT é o de proporcionar ao comandante informação sobre as capacidades do inimigo ou terceiros, o seu dispositivo e intenções. Adicionalmente, as SIGINT também fornecem informações úteis para o *targeting* permitindo bater, de forma mais precisa, o inimigo ou terceiros, com meios letais e não-letais.

Normalmente, os meios SIGINT pertencem aos mais altos escalões da componente terrestre, a outras componentes e departamentos governamentais. Assim, todos estes meios trabalharão em conjunto para apoiar os comandantes desde o nível tático até ao nível estratégico.

Igualmente importante, é diferenciar a SIGINT das Medidas de Apoio Electrónico (ESM – *Electronic Support Measures*), enquanto uma das actividades da Guerra Electrónica (EW – *Electronic Warfare*). Estas têm como finalidade a obtenção de informação para o apoio ao planeamento e conduta das operações militares ao nível operacional/tático e têm uma execução limitada no tempo e no espaço, enquanto que a SIGINT, podendo usar os mesmos procedimentos e equipamentos que as ESM, visa a obtenção de informação para os utilizadores, desde o nível político/estratégico, até aos comandantes militares operacionais ou táticos, possibilitando assim, quer o planeamento em tempo de paz, de longo prazo (Planeamento da Defesa Nacional), quer o apoio de curto prazo a operações militares (em situações de crise ou guerra).

0208. Informação de Medição e Assinatura Electromagnética

A MASINT é informação científica e técnica obtida pela análise quantitativa e qualitativa dos dados (métricos, espaciais, comprimento de onda, dependência do tempo,

modulação, plasma e hidromagnético, etc.), provenientes de objectos/alvos e fontes fixas ou dinâmicas, que contribui para a sua detecção, localização, seguimento, identificação e/ou descrição. Inclui também o processamento e exploração avançados de dados com origem na pesquisa IMINT e SIGINT.

Os meios de MASINT incluem meios de espectroradiometria de radar, meios electro-ópticos, acústicos, radiofrequência, sensores sísmicos, bem como as técnicas e equipamentos para detecção Nuclear, Biológica, Química e Radiológica (NBQR).

A MASINT fornece ao comandante informação que facilita o conhecimento da situação operacional, pois pode contrariar muitas das actuais técnicas de camuflagem, ocultação e decepção inimiga.

A MASINT é uma disciplina de nível estratégico, com uma limitada capacidade de apoio ao nível tático, mas através da aplicação em tempo quase real da análise e disseminação da informação, tem o potencial de contribuir para a avaliação da situação operacional e para o *targeting*.

Os sensores MASINT têm capacidades únicas na detecção do lançamento de mísseis, detecção e seguimento de aeronaves, navios e veículos; na identificação não-cooperativa de alvos, BDA; e na detecção e localização de detonações nucleares. Estas actividades são muitas vezes os primeiros indicadores de actuação hostil.

A MASINT inclui:

a. Informação de Radares (RADINT - *Radar Intelligence*)

A RADINT é a informação obtida pela utilização de radares como principal meio de pesquisa e aquisição.

Os meios de pesquisa RADINT fornecem informação sobre a capacidade de re-radiação ou assinatura radar, de seguimento, medição espacial precisa de componentes, de movimento, de reflexão radar e características de absorção de objectos e alvos dinâmicos.

b. Informação Acústica (ACINT - *Acoustic Intelligence*)

A ACINT é a informação obtida através da pesquisa e análise de fenómenos acústicos. Exemplos de fontes ACINT são: hidrofones, geofones, sonares, sistemas integrados de vigilância subaquática (IUSS - *Integrated Underwater Surveillance System*) e sistemas acústicos de artilharia (bases de som). Dada a natureza do fenómeno acústico, a ACINT é principalmente adequada ao meio aquático e à detecção de movimentos.

SECÇÃO III – ÁREAS FUNCIONAIS DAS INFORMAÇÕES

0209. Generalidades

As áreas funcionais das informações compreendem assuntos específicos da produção de informações e que exigem, normalmente, a análise por especialistas. Contribuem para a produção das informações em geral, dando origem a informações concretas, que respondem a necessidades específicas dos utilizadores. Estas áreas funcionais são transversais às várias disciplinas das informações, podendo incluir, entre outras, as seguintes informações:

- Biográficas;
- Económicas;
- Engenharia;
- Forças Armadas;
- Geoespacial;
- Infra-estruturas;
- Logísticas;
- Médicas;
- Políticas;
- Segurança;
- Sociológicas;
- *Targeting*;
- Técnicas e Científicas;
- Técnicas.

0210. Informações Biográficas

São as informações sobre os pensamentos, hábitos, qualificações, aptidões, importância, relacionamento, estado de saúde e *curriculum vitae* sobre qualquer pessoa, com interesse actual ou potencial para as informações.

0211. Informações Económicas

São as informações respeitantes a recursos económicos, actividades e políticas de entidades estrangeiras, incluindo a produção, distribuição e consumo de bens e serviços, emprego, finanças e outros aspectos do sistema económico internacional, tais

como o comércio e investimento.

0212. Informações de Engenharia

São o produto do processamento da informação referente às operações de engenharia inimigas, recursos, condições ambientais, informação geográfica militar e terreno, necessárias ao comandante para o planeamento das operações de combate.

0213. Informações sobre Forças Armadas

São as informações relativas a todos os aspectos das forças terrestres, navais, aéreas e espaciais inimigas ou potenciais, incluindo a ordem da batalha, comando e controlo, sistemas de armas, treino, pessoal, doutrina, estratégia e táticas, logística, negócios de armamento, indústrias de defesa e despesas com a defesa.

0214. Informações Geoespaciais

As informações geoespaciais consistem na exploração e análise das imagens de satélite, que visualizam, avaliam e descrevem os aspectos físicos e geográficos da área analisada.

0215. Informações sobre Infra-Estruturas

São as informações respeitantes à rede ferroviária, estradal, de *pipelines*, de distribuição de água e sistemas de telecomunicações.

0216. Informações Logísticas

São as informações respeitantes à capacidade de movimentar forças, apoiar e sustentar operações militares.

0217. Informações Médicas

As informações médicas são as obtidas em resultado do processamento médico, bio-científico, epidemiológico, ambiental e outra informação relacionada com a saúde humana ou animal. Esta informação, sendo de natureza técnica específica, exige peritos da área de saúde durante as fases de orientação do esforço de pesquisa e processamento do ciclo da produção da informação.

0218. Informações Políticas

São as informações a respeito da dinâmica dos casos políticos internos e externos de

PDE 2-00 Informações, Contra-Informação e Segurança

países estrangeiros, grupos regionais, acordos e tratados multilaterais, e movimentos políticos estrangeiros de apoio ou contestação a governos e autoridades estabelecidos. Inclui estruturas do governo, políticas internas e estrangeiras.

0219. Informações de Segurança

As Informações de Segurança (SI – *Security Intelligence*) são definidas como informações sobre a identidade, potencialidades e intenções de organizações hostis ou indivíduos que estão ou podem vir a estar envolvidos em actividades de espionagem, sabotagem, subversão ou terrorismo. Estas organizações ou indivíduos são, ou podem vir a ser, uma ameaça em tempo de paz, em situações de emergência ou conflito, à segurança de recursos, actividades, operações, pessoal e informações de nações e de forças da Organização do Tratado do Atlântico Norte (OTAN). Inclui as informações sobre serviços de informações estrangeiros e crime organizado. Relaciona-se especialmente com a actividade de contra-informação (CI – *Counter-Intelligence*).

0220. Informações Sociológicas

São as informações respeitantes aos factores de ordem social e cultural, incluindo dados sobre a população, etnias, estratos e estabilidade social, opinião pública, instrução, religião, saúde, história, língua, valores, percepções e comportamento.

0221. Informações sobre *Targeting*

São as informações que permitem enquadrar e localizar os componentes de um objectivo ou de um conjunto de objectivos; indicando a sua identificação, vulnerabilidades e importância relativa.

0222. Informações Técnicas e Científicas

As Informações Técnicas e Científicas (STI - *Scientific and Technical Intelligence*) são as informações sobre as inovações verificadas no estrangeiro, no que diz respeito à investigação e desenvolvimento técnico e científico, incluindo técnicas de engenharia e de produção, novas tecnologias, sistemas de armas e suas capacidades.

0223. Informações Técnicas

As Informações Técnicas (TECHINT - *Technical Intelligence*) são as informações relativas a desenvolvimentos tecnológicos estrangeiros e das capacidades operacionais do equipamento estrangeiro que têm, ou podem vir a ter, uma aplicação prática para

fins militares. Esta informação resulta do exame e de testes científicos ao equipamento, incluindo o *hardware* e o *software* dos computadores. Os testes visam determinar as potencialidades e limitações dos equipamentos adversários e apoiar o desenvolvimento das contramedidas a aplicar a esses equipamentos. As TECHINT são uma subdivisão das STI.

Página intencionalmente em branco

CAPÍTULO 3 O CICLO DA PRODUÇÃO DA INFORMAÇÃO

SECÇÃO I – GENERALIDADES

0301. O Ciclo da Produção da Informação

Tendo em vista o tratamento de todas as notícias disponíveis, existe a necessidade de realizar uma série de fases sistemáticas e estruturadas a fim de identificar a que é relevante, pesquisar a omissa ou inexistente e processar aquela que se julga necessária, que irá dar origem às informações.

O Ciclo da Produção da Informação é uma sequência das actividades de informações na qual a notícia é obtida, transformada em informação e explorada. Esta sequência compreende quatro fases distintas (**orientação do esforço de pesquisa** (a que também se pode chamar direcção), **pesquisa**, **processamento** e **disseminação**) que culmina na distribuição do produto acabado. Cada fase do ciclo deve ser sincronizada com o processo de decisão do comandante e as necessidades da operação de forma a poder influenciar com sucesso o resultado da operação. O Ciclo da Produção da Informação é uma forma de entender e coordenar as várias actividades envolvidas na produção de informações, auxiliando a compreender as inter-relações existentes nas várias fases. O processo de produção das informações pode ser interrompido durante o seu ciclo e não existem limites rígidos a delimitar os pontos em que cada fase do ciclo se inicia ou conclui. As fases ou passos do ciclo são mostradas no diagrama da Figura 3-1:

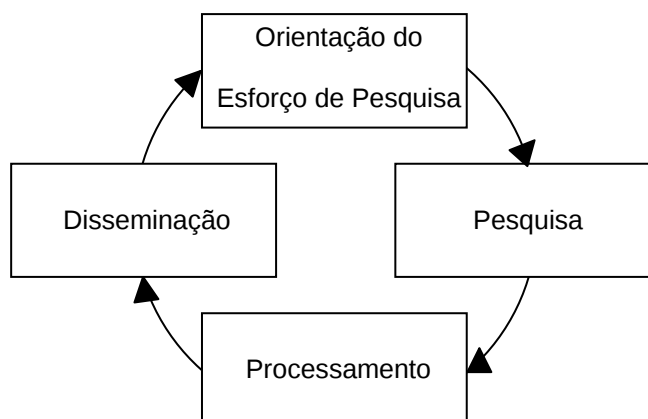


Figura 3-1 – O Ciclo da Produção da Informação

0302. Definições

Para que o comandante e o seu estado-maior possam orientar o seu esforço de informações, são definidas as Áreas de Responsabilidade de Informações (AIR - *Areas of Intelligence Responsibility* e Áreas de Interesse (AOI - *Areas of Interest*), em relação à Área de Operações (AOO – *Area of Operations*). Estas áreas podem não ser só geoespaciais, podendo incluir outros factores tais como políticos, demográficos, económicos ou ciberespaço.

a. Área de Operações

A AOO é uma área definida pelo comandante das forças conjuntas para as forças terrestres e navais para conduzir as operações militares e a sua administração. Normalmente, as áreas de operações não envolvem toda a área operacional do comandante das forças conjuntas, mas devem ser suficientemente extensas para permitir aos comandantes de componente o cumprimento da missão e a protecção da força.

b. Área de Responsabilidade de Informações

A AIR é definida como a área geográfica atribuída a um comandante, na qual este é o responsável pela obtenção de informações, de acordo com os meios à sua disposição. Na prática, a dimensão desta área será limitada pelas capacidades dos meios de pesquisa à sua disposição, das quais o alcance e acesso serão os principais factores. Ambos os factores influenciarão a área na qual o comandante orientará o esforço da célula de informações.

c. Área de Interesse

A AOI pode ser definida como a área de preocupação de um comandante, para além da AOO, onde a existência de factos e acontecimentos ou a provável ocorrência de actividades possam vir a afectar as operações correntes ou futuras. Caso não consiga obter essas informações com os seus meios de pesquisa, terá que as solicitar ao escalão superior ou às unidades adjacentes. As notícias e informações obtidas fora da AIR devem ser disseminadas para todas as unidades a quem possam interessar. A AOI pode ser definida em termos de espaço e tempo. A relação entre as áreas é mostrada no diagrama da Figura 3-2.

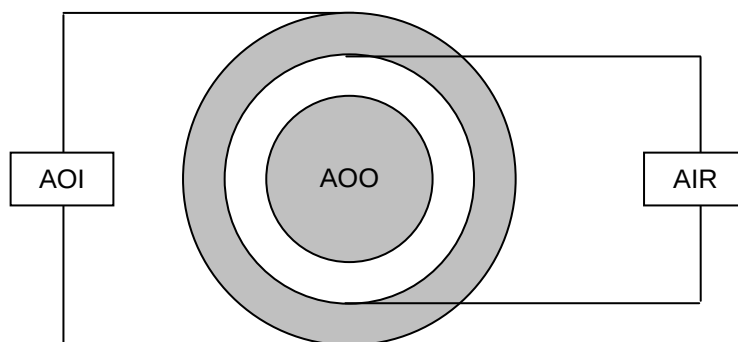


Figura 3-2 – Relações entre AOO, AIR e AOI

SECÇÃO II – ORIENTAÇÃO DO ESFORÇO DE PESQUISA

0303. Definição

A orientação do esforço de pesquisa é a primeira fase do Ciclo da Produção da Informação e consiste na determinação das necessidades de informações, no planeamento do esforço de pesquisa, na emissão de ordens e pedidos aos órgãos de pesquisa e na manutenção de uma contínua verificação da sua produtividade.

A orientação do esforço de pesquisa compreende:

- a. **A que é dada pelo comandante à sua célula de informações.** O comandante deve orientar a célula de informações através de instruções claras sobre as notícias e informações que necessita, estabelecendo um limite de tempo para a sua obtenção. A sua orientação deve ser a mais específica possível, atribuindo prioridades às necessidades de informação. Além disso, deve indicar quando as mesmas são necessárias, a frequência dos relatórios e a precisão necessária para o *targeting*.
- b. **A que é dada pela célula de informações às suas origens e órgãos.** Esta orientação é a base do Plano de Pesquisa e inclui:
 - (1) A decisão de como serão respondidas as questões do comandante e que notícias e informações são necessárias para o fazer.
 - (2) A garantia de que as informações não estão localmente disponíveis antes de atribuir tarefas às origens e órgãos orgânicos.
 - (3) A atribuição de tarefas às origens e órgãos para pesquisa necessária.

- (4) A monitorização da pesquisa de forma a garantir que a informação adequada é pesquisada.

0304. Necessidades de Informação Crítica do Comandante

- a. No decorrer de uma operação, possivelmente ainda antes da fase de projecção, o comandante formulará as questões para as quais necessita de resposta, de forma a conduzir a operação com sucesso. Estas questões são as Necessidades de Informação Crítica do Comandante (CCIR - *Commander's Critical Information Requirements*) e dizem respeito ao estado de operacionalidade e capacidades de forças amigas, ao estado de operacionalidade, capacidades e intenções do inimigo e características da área de operações.
- b. O comandante designa as CCIR para que o estado-maior e os seus subordinados saibam qual a informação que ele julga necessária para a tomada de decisão e para orientarem os seus esforços de pesquisa. Quanto menor for o número de CCIR, melhor o estado-maior pode orientar os seus esforços e atribuir os recursos.
- c. O comandante decide qual é a informação fundamental, com base nas suas capacidades cognitivas e na sua visão. O estado-maior pode auxiliar o comandante ao recomendar CCIR, com base na análise das operações. As CCIR não são estáticas; o comandante ajusta e actualiza-as ao longo da operação, de modo a reflectir novas necessidades de informação para a tomada de decisão, à medida que a operação decorre. As CCIR são:
 - definidas pelo comandante para cada operação;
 - aplicáveis apenas ao comandante que as define;
 - dependentes da situação – directamente ligados a missões correntes e futuras;
 - actividades e acontecimentos previsíveis;
 - sensíveis a factores temporais. As respostas aos CCIR têm de ser imediatamente transmitidas ao comandante;
 - sempre incluídas numa Ordem ou Plano de Operações.

- d. As CCIR orientam a informação transmitida ao comandante e são fundamentais para a sua tomada de decisão. As respostas aos CCIR devem determinar ou validar uma modalidade de acção ou iniciar acontecimentos críticos durante as operações.
- e. As CCIR compreendem as Necessidades Prioritárias de Informações (PIR - *Priority Intelligence Requirements*) e as Necessidades de Informação sobre Forças Amigas (FFIR - *Friendly Forces Information Requirements*). As PIR e os FFIR podem incluir o Tempo de Validade da Informação (LTIOV - *Latest Time Information Of Value*) para orientar o tempo de pesquisa (figura 3.3).

0305. Necessidades Prioritárias de Informações

Muitas das questões contidas nas CCIR apenas exigirão factos e podem ser respondidas pela pesquisa e disseminação de informação. Haverá, contudo, algumas questões relativamente às características da área de operações e ao inimigo que são críticas para o planeamento e execução com sucesso das modalidades de acção amigas e que necessitam de ser processadas em informações para dar resposta a essas questões. As PIR são apenas aquelas necessidades de informações para as quais o comandante antecipadamente definiu uma prioridade no decurso do processo de decisão. Consistem na informação mais importante que o comandante e o estado-maior necessitam de saber acerca do inimigo, quais as suas intenções, capacidades operacionais (incluindo o tempo disponível para o inimigo) e o meio envolvente (terreno, condições meteorológicas e considerações civis); ou seja, como se visualiza o inimigo.

0306. Necessidades de Informação sobre Forças Amigas

As FFIR consistem na informação de que o comandante e o estado-maior precisam de saber acerca das nossas forças disponíveis para a operação. As FFIR garantem informação acerca da missão, unidades, tempo disponível, grau de operacionalidade e instrução, ou seja, como me visualizo.

0307. Elementos Essenciais de Informação das Forças Amigas

Os Elementos Essenciais de Informação das Forças Amigas (EEFI – *Essential Elements of Friendly Information*) são os aspectos fundamentais de uma força amiga que, se forem conhecidos do inimigo, comprometem o cumprimento de uma missão, tendo de ser protegidos da pesquisa inimiga; ou seja, como é que se pode evitar que a força inimiga nos veja. Apesar de os EEFI não fazerem parte das CCIR, tornam-se em

PDE 2-00 Informações, Contra-Inteligência e Segurança

prioridades do comandante quando ele os declara. Tal como as CCIR, o comandante designa os EEFI e transmite-os ao estado-maior e aos Comandantes subordinados. Estes dizem ao comandante o que é que não pode ser detectado pelo inimigo. Se assim for determinado, as forças amigas têm de tomar todas as medidas necessárias para assegurar que esta informação não vai ser do conhecimento do inimigo. Por exemplo, um comandante poderá determinar que se o inimigo descobrir o movimento da reserva, a operação está em risco. Nesse caso, a localização e o movimento da reserva torna-se num EEFI. Os EEFI são essenciais para as INFO OPS, uma vez que são muitas vezes elementos-chave na definição de operações militares de decepção e medidas de Segurança das Operações (OPSEC – *Operations Security*).

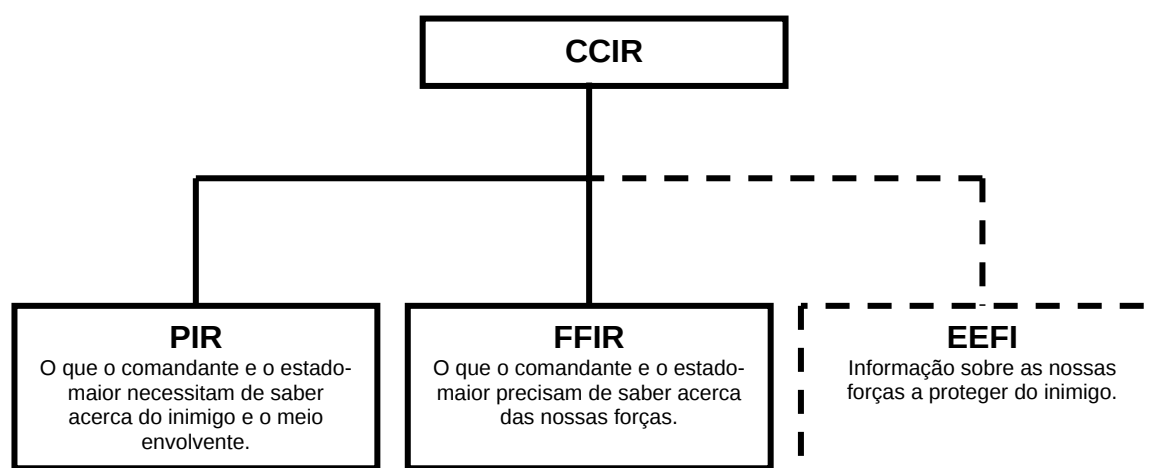


Figura 3-3 – Necessidades de Informação Crítica do Comandante

0308. Necessidades de Informação

Os PIR são divididos em necessidades de informação individual que, quando processadas e integradas, respondem aos PIR. As necessidades de informação (IR – *Information Requirements*), que também podem ser designados por quesitos concretos, são definidas como aqueles itens de informação a respeito das características da área de operações e do inimigo que precisam de ser pesquisados e processados para responder às necessidades de informação do comandante.

0309. Indicadores

Para atribuir as tarefas aos meios de pesquisa, a Célula de Informações tem de identificar os indicadores mais adequados para cada necessidade de informação. Em alguns casos, a identificação desses indicadores pode exigir apoio ou especialistas de origens ou órgãos externos. Os indicadores, que também podem ser designados por

indícios técnicos, são definidos como manifestações, positivas ou negativas, da actividade inimiga ou qualquer aspecto específico da área de operações que podem revelar determinada vulnerabilidade do inimigo, indicar a adopção ou rejeição (pelo inimigo) de determinadas modalidades de acção ou influenciar a escolha (pelo comandante) de uma modalidade de acção. São agrupados da seguinte forma:

- a. **Indicadores de Alerta e Aviso.** Os relacionados com os preparativos de agressão por parte de um inimigo, alguns dos quais darão um aviso oportuno da iminência das hostilidades.
- b. **Indicadores de Combate ou Táticos.** Estes indicadores revelam o tipo de operação que o inimigo está prestes a realizar. Cada tipo de operação vai obrigar a uma preparação específica e característica. Os indicadores ligados a estas preparações podem ser definidos antes das operações e ligados a tipos de operações específicas.
- c. **Indicadores de Identificação.** São aqueles que permitem a identificação e acção de uma formação, unidade ou instalação, a partir do conhecimento da sua organização, equipamento e táctica.

A selecção dos indicadores apropriados à situação operacional irá depender em grande medida das capacidades e experiência da célula de informações. A natureza dos indicadores vai originar a escolha de origens e órgãos encarregados de recolher a informação necessária para responder às necessidades de informações.

0310. Conceito de Gestão das Necessidades de Informações e Coordenação da Pesquisa

O planeamento da pesquisa de informações pode ser iniciado assim que os PIR começam a ser identificados. A melhor metodologia para elaborar o plano de pesquisa e gerir a sua execução de forma mais eficaz é a Gestão das Necessidades de Informações e Coordenação da Pesquisa (CCIRM - *Collection Coordination and Intelligence Requirements Management*). O segredo para responder aos CCIR e PIR reside na elaboração de um plano de pesquisa eficaz, de acordo com os princípios das informações.

PDE 2-00 Informações, Contra-Informação e Segurança

A CCIRM engloba aquelas actividades que resultam num emprego eficiente e eficaz da pesquisa, processamento, exploração e disseminação de informações para satisfazer as necessidades de informações aos níveis tático, operacional e estratégico e nacional. A CCIRM compreende dois componentes² principais: a coordenação da pesquisa e a gestão das necessidades de informações que resultam de operações ou missões. Uma arquitectura de informações eficaz permitirá uma atribuição e reatribuição rápida e eficiente das tarefas às origens e órgãos.

SECÇÃO III – PESQUISA

0311. Introdução

A pesquisa é a segunda fase do Ciclo da Produção da Informação. É definida como a exploração dos meios pelas origens e órgãos de pesquisa e a entrega da informação obtida à unidade de processamento apropriada para produção de informações. É o processo no qual as informações são pesquisadas para responder às necessidades de informações do comandante, identificadas na fase de orientação do esforço de pesquisa do Ciclo da Produção da Informação.

O processo de pesquisa divide-se em três partes:

- a. Gestão das necessidades de pesquisa através do desenvolvimento e execução de um plano de pesquisa.
- b. A exploração dos meios pelas origens e órgãos de pesquisa pela célula de informações;
- c. A entrega oportuna das notícias pesquisadas pelas origens e órgãos à fase seguinte do Ciclo da Produção da Informação, onde esta será processada em informações.

² Explicado em detalhe no Capítulo 4. As actividades de CCIRM ocorrem na ordem inversa do acrónimo em inglês. Ou seja, a Gestão das Necessidades de Informações ocorre antes da Coordenação da Pesquisa.

0312. Princípios da Pesquisa

A pesquisa é orientada pelos seguintes princípios:

a. Orientação Precisa

Devem ser dadas orientações precisas às origens e órgãos, de forma a se obter a informação desejada.

b. Coordenação Centralizada

Só através de uma coordenação centralizada se consegue utilizar da forma mais adequada os vários órgãos de pesquisa. Esta centralização é normalmente conseguida ao mais alto escalão, de forma a garantir a utilização mais eficaz das capacidades de cada meio.

c. Tempo e Espaço

O tempo e o espaço são os aspectos mais importantes para a atribuição dos meios de pesquisa. Estes, por serem sempre escassos, devem ser empregues de forma eficiente, de modo a cobrir todo o espaço de batalha. Isto implica a necessidade de priorizar e ordenar as necessidades de informação.

d. Capacidade

Na selecção dos meios de pesquisa devem ser consideradas as seguintes características:

(1) Segurança e Risco

O meio de pesquisa deve ser protegido de forma adequada, mantendo a capacidade de recolher a informação necessária. Existirá sempre um risco físico, político ou militar na utilização de qualquer meio de pesquisa, que deverá ser ponderado, tendo em conta o risco da perda do meio e o ganho de informações. Da mesma forma, o facto de um meio de pesquisa poder indicar ao inimigo o que está a ser pesquisado, pode ser também um indício das nossas intenções.

(2) O Ambiente das Operações

A natureza do ambiente em que decorrem as operações, como por exemplo as condições meteorológicas, o terreno, ou constrangimentos políticos, pode limitar a capacidade de obtenção de informação de um meio de pesquisa. Dependendo da importância para o sucesso da pesquisa, podem ser utilizados

PDE 2-00 Informações, Contra-Informação e Segurança

meios de pesquisa alternativos como contingência face a mudanças no ambiente geoespacial.

(3) Redundância

É um processo deliberado que utiliza mais de um meio para pesquisar o mesmo objectivo. Vários meios de pesquisa devem operar em sobreposição no espaço de batalha, garantindo a redundância. A escassez de meios de pesquisa pode limitar este processo, o que exige uma coordenação a todos os níveis de comando.

0313. A Exploração de Origens e Órgãos

A diferença principal entre uma origem e um órgão reside no facto da primeira produzir exclusivamente dados e notícias, ao passo que o segundo, para além da capacidade de pesquisa, possui também alguma capacidade de processamento, produzindo informações. As origens e órgãos são definidos como:

a. Origem

As origens de notícias são as fontes (pessoas, coisas ou acções) de que provêm todas as notícias pesquisadas acerca do inimigo e da área de operações.

b. Órgão

Um órgão de pesquisa é qualquer indivíduo, entidade ou unidade que obtém ou processa notícias.

0314. Tipos de Origens e Órgãos

As origens e órgãos podem ser agrupados da seguinte forma:

a. Controlados

Origens e órgãos aos quais um oficial de informações pode atribuir tarefas para obtenção das respostas às suas questões. Incluem, por exemplo, Sistemas de Informações, Vigilância, Aquisição de Objectivos e Reconhecimento (ISTAR - *Intelligence, Surveillance, Target Acquisition and Reconnaissance*) terrestres e aéreos, tripulações de navios, veículos terrestres e aéreos.

b. Não Controlados

Origens e órgãos que fornecem informações mas que não estão sob controlo de um oficial de informações e aos quais não podem ser atribuídas tarefas. São exemplo de origens e órgãos não controlados os jornais, rádios, televisões, mapas e cartas

produzidas por governos hostis ou neutrais. Fazem parte, também, desta categoria, os sistemas de vigilância estratégica operados por nações amigas. Apesar do conteúdo destes meios poder estar disponível, a sua programação estará sobre o controlo das nações que os possuem e as restantes nações não podem interferir no seu uso.

c. Ocasionais

Uma origem ocasional produz informação de forma irregular. Um exemplo de uma origem ocasional pode ser um traidor ou refugiado. Os dados de uma origem ocasional devem ser tratados com precaução pois podem fazer parte de um plano de decepção do inimigo.

A célula de informações deve ter conhecimento, directo ou através de representantes dos órgãos, das capacidades de todas as origens e órgãos que têm à sua disposição. Isto irá permitir a selecção adequada de uma origem ou órgão, para uma tarefa específica de pesquisa, e monitorizar o grau de confiança e produtividade das origens e órgãos utilizados.

0315. Selecção de Origens e Órgãos

Na selecção de uma origem ou órgão para uma tarefa específica, para além dos princípios da pesquisa, deve ter-se em consideração os seguintes factores:

a. Segurança

De acordo com os princípios das informações, as origens e órgãos devem ser protegidos de forma adequada. Uma falha na segurança poderá resultar na perda da origem ou órgão ou o seu comprometimento e possível uso para introduzir informação de decepção no canal de informações.

b. Capacidade

A origem escolhida para a pesquisa de um item específico de informação deve ser capaz de cumprir essa tarefa. Aos meios humanos são atribuídas tarefas de recolha de informação, como é dever intrínseco do militar que circula no TO, mas não lhe podem ser atribuídas tarefas de HUMINT. Estas só poderão ser atribuídas à posteriori aos Operadores de HUMINT especializados, com a informação que tiver sido obtida numa primeira recolha. O órgão a que é atribuída a tarefa de pesquisar uma determinada informação deve ser possuidor das capacidades necessárias para a sua execução, dispondo como tal de sistemas, de sensores e/ou capacidade de processamento, de obter notícias e/ou produzir informações em formato

PDE 2-00 Informações, Contra-Informação e Segurança

adequado. Deve-se manter um registo de tarefas semelhantes às realizadas, com sucesso, no passado.

c. Aptidão

Haverá ocasiões em que mais de um tipo de origem ou órgão são capazes de executar determinada tarefa de pesquisa e estão disponíveis para o fazer. Para decidir quem irá executar o quê, devem ser tidas em consideração as capacidades e limitações de cada um, de forma a assegurar que o meio escolhido é o mais adequado.

0316. Entrega da Informação

As notícias e informações perdem rapidamente o seu valor com o tempo. De forma a minimizar essa degradação, o tempo do Ciclo da Produção da Informação deve ser o mais reduzido possível. Assim, é um requisito essencial de uma origem ou órgão ser capaz de enviar as notícias ou informações pesquisadas no mais curto espaço de tempo, dentro de uma janela de tempo definida pela entidade que lhe atribui a tarefa. Neste contexto, existem dois conceitos:

a. Tempo de Resposta

Tempo de resposta é o intervalo de tempo entre o pedido de informação e a recepção da resposta. O tempo de resposta de um sistema de pesquisa depende do tipo de origem ou órgão empregue. Se para cumprir essa tarefa for empregue um sistema como uma aeronave não-tripulada (UAV – *Unmanned Aerial Vehicle*) ou uma aeronave tripulada, o tempo de projecção desse sistema aumenta significativamente o tempo de resposta. Se, no entanto, a origem já estiver projectada, como é o caso de um satélite, de uma aeronave com um sistema de radar (ASTOR - *Airborne Stand Off Radar*), ou um sistema de pesquisa de Informação de Transmissões Electromagnéticas e Comunicações (SIGINT - *Signals Intelligence*), o tempo de resposta global será muito inferior.

b. Tempo de Relato

O tempo de relato é o intervalo de tempo entre a detecção de um item de informação por um sensor e a sua recepção por um analista. O valor e confiança da maioria da informação pesquisada para uso ao nível tático decrescem rapidamente com o passar do tempo. O LTIOV deve ser definido no plano de pesquisa. O desejável é que a informação chegue ao analista quase em tempo real; no entanto, isso depende do estabelecimento de uma ligação directa entre o sensor

e o analista. Infelizmente, esta ligação directa apenas existe nos sistemas mais sofisticados. O tempo de relato para a maioria das origens e órgãos pode variar bastante e deve ser tomado em consideração na escolha de uma origem ou órgão para a execução de uma dada tarefa. Alguns dos factores que afectam o tempo de relato das origens e órgãos são os seguintes:

- (1) A necessidade de recuperar o sensor para a base de origem do seu sistema de transporte, tal como o de um equipamento de reconhecimento fotográfico.
- (2) A necessidade de a informação passar por um processo de transformação (alteração do formato) para ser legível, tal como a revelação de um filme fotográfico.
- (3) A disponibilidade de sistemas de comunicações e largura de banda suficiente para transmissão de dados.

0317. A Natureza do Plano de Pesquisa

O plano de pesquisa deve ser visto como um processo contínuo que atribui ou reatribui tarefas às origens e órgãos, de acordo com as necessidades de informação. Isto acontece à medida que a operação decorre e nalguns casos, resulta das notícias e informações das tarefas iniciais.

SECÇÃO IV – PROCESSAMENTO

0318. Introdução

O processamento é a parte do Ciclo da Produção da Informação em que as notícias que foram pesquisadas, em resposta à orientação do comandante, são convertidas em informações. O processamento é uma série estruturada de acções as quais, apesar de elaboradas em sequência, podem também ocorrer em simultâneo. O processamento é definido como a transformação de notícias em informações através do registo, avaliação, análise, integração e interpretação.

O processamento é feito ao longo das diversas fases do Ciclo da Produção da Informação. Tal pode ir desde o processamento inicial levado a cabo num órgão de pesquisa, o que geralmente não envolve mais do que a alteração do formato dos dados em bruto para uma forma inteligível, ao processamento de informações que tenham passado pela cadeia de comando, ao nível estratégico. Cada novo processamento relaciona a notícia ou informação aos factos que não estavam disponíveis nos níveis de processamento anteriores, permitindo assim a dedução de novas informações. O

PDE 2-00 Informações, Contra-Informação e Segurança

processamento divide-se em cinco partes, sendo elas o **registo**, a **avaliação**, a **análise**, a **integração** e a **interpretação**.

0319. Registo

O registo é um passo na fase de processamento do Ciclo da Produção da Informação, que consiste no agrupamento sistemático de todas as notícias, criando um registo de acontecimentos, de forma a facilitar a sua ulterior transformação em informações e a elaboração de documentos de informações. Na prática, é composto pelos procedimentos de recepção, agrupamento e registo de todos os relatórios que chegam a uma célula de informações a qualquer nível e envolve a:

- a. Tarefa básica de atribuir um número de identificação e registar a recepção de qualquer notícia e informação recebida.
- b. Colocação adequada da notícia e informação numa categoria ou grupo num diário, carta de situação, pasta de trabalho, arquivos de informações ou em base de dados electrónica.
- c. Manutenção de um sistema para condução destas operações, desenhado de forma a que qualquer membro da célula de informações o possa operar com rapidez e eficiência.

Aos mais baixos escalões, o registo pode resumir-se a uma pasta de arquivo e a uma actualização da carta de situação. No entanto, à medida que aumenta o escalão, o sistema de registo torna-se mais sofisticado, envolvendo sistemas de tecnologias de informação, ecrãs, circuitos fechados de televisão, sistemas para brifings, bases de dados electrónicas e sistemas de transmissão de dados de alta velocidade. Como princípio básico, devem ser empregues, sempre que possível, ecrãs de representação gráfica para auxiliar a respectiva célula de informações na obtenção da maior quantidade de informação no mais curto espaço de tempo possível.

As categorias ou grupos em que será colocada a informação pelo sistema de registo, deve estar relacionada com as AIR das unidades e o tipo de operações a executar. Também devem ser baseadas:

- nas necessidades de informações do comandante;
- nas necessidades de informações das células de informações e operações;
- no volume de informação esperado para o sistema.

0320. Factores que Afectam o Registo

Quando se estabelece e opera um sistema de registo devem ser tidos em consideração os seguintes factores:

a. Normalização

Sempre que possível, os títulos e subtítulos do assunto dos grupos em que a informação é colocada nos sistemas de registo individual das unidades, deve estar de acordo com uma norma definida pela célula de informações do quartel-general do escalão mais elevado. A utilização pelas células de informações dos mesmos títulos de assunto para a categorização das informações e de uma estrutura normalizada de bases de dados de informações, simplifica e aumenta a velocidade do processamento, facilitando a troca de informações entre as unidades.

b. Títulos e Subtítulos de Assunto Comuns

A selecção dos títulos e subtítulos para os grupos deve ser baseada nos IR associados ao tipo de operação a executar, bem como ao ambiente do espaço de batalha. Uma selecção cuidada dos títulos e subtítulos torna mais rápida e directa a categorização das notícias e informações.

c. A Importância da Referenciação Cruzada

Todas as entradas no sistema devem ser cruzadas com o relatório original e com outras entradas no sistema, no arquivo e no índice. Quando são utilizadas bases de dados electrónicas, este trabalho de natureza relacional é executado automaticamente.

d. Apresentação Visual

A utilização de mapas, gráficos, diagramas e apresentações em ecrãs, deve ser explorado como um meio auxiliar para uma mais rápida e fácil assimilação de grandes quantidades de notícias e informações.

e. Urgência e Rapidez de Reacção

O sistema deve ter a capacidade de reagir rapidamente a pedidos imediatos para o processamento de notícias e informações necessárias de modo a responder às necessidades do comandante.

f. Restrições no Volume de Registos

A capacidade do sistema em tratar um grande volume de registos em termos de armazenamento e processamento será ditado pelo:

- (1) Número de elementos da célula de informações disponível para operar o sistema.
- (2) Natureza e ritmo das operações.
- (3) Capacidade de armazenamento do equipamento.
- (4) Capacidade de arquivo e recuperação do sistema.
- (5) Espaço disponível na célula de informações.
- (6) Dimensão e objectivo da tarefa de informações.

g. Pragmatismo

Haverá sempre a tentação de processar toda a notícia e informação que chegam à célula de informações. Isto provocará uma sobrecarga do sistema e dos procedimentos, tornando-os lentos ou, no pior dos cenários, bloqueará o sistema e deixará de produzir informações. Para o evitar, tem que se encontrar um compromisso entre o desejável e o possível. Tal pode ser conseguido através da adopção de uma abordagem pragmática ao processo de pesquisa, purgando constantemente o sistema, actualizando os registos e filtrando cuidadosamente o material recebido, para que só seja processada e enviada para a fase seguinte a informação relevante para as necessidades de informações imediatas.

h. Prioritização

O pessoal encarregue do registo deve estar consciente das prioridades das várias necessidades de informações para que estas sejam relacionadas de acordo com as prioridades e processadas com o adequado grau de urgência.

0321. Avaliação

A avaliação é um dos passos da fase de processamento do Ciclo da Produção da Informação que consiste na apreciação de um item de informação relativamente ao grau de confiança da origem ou órgão de pesquisa e ao grau de verosimilhança da notícia. De forma sucinta, é uma avaliação de quanto a origem é de confiança e de quanto é provável que a notícia seja verdadeira. A notícia recebida não pode ser considerada pelo seu valor aparente. Existem muitas razões, não apenas a decepção, para que uma

notícia não seja credível ou totalmente verosímil. O passo da avaliação atribui uma escala alfanumérica a cada notícia que indica a classificação da mesma.

A atribuição desta escala é baseada por um lado no julgamento subjectivo do avaliador, por outro lado na experiência acumulada de outras informações colhidas pela mesma origem e ainda, no caso de dados obtidos através de sensores, no conhecimento da precisão desses sistemas. A confiança da origem e a verosimilhança da notícia devem ser avaliadas independentemente uma da outra, para garantir que a atribuição de um valor na confiança não influencia o valor da credibilidade, ou vice-versa. A informação que é produzida por uma origem de confiança não é necessariamente correcta, nem a notícia que se demonstra ser verdadeira significa que a origem é de confiança.

Os valores para atribuição da classificação para o grau de confiança da origem ou do órgão e a verosimilhança da notícia são os seguintes:

Confiança da Origem ou do Órgão		Verosimilhança da Notícia	
A	Absolutamente seguro	1	Confirmada por outras origens
B	Normalmente seguro	2	Provavelmente verdadeira
C	Razoavelmente seguro	3	Possivelmente verdadeira
D	Normalmente não seguro	4	Duvidosa
E	Não seguro	5	Improvável
F	Não pode ser apreciado	6	Não pode ser determinada

As classificações são atribuídas combinando os graus. Assim, por exemplo, a notícia julgada com “Provavelmente verdadeira” de um órgão conhecido como sendo “Normalmente seguro” terá a classificação de B2. Por outro lado, uma notícia cuja verosimilhança “Não pode ser determinada” obtida pelo mesmo órgão “Normalmente seguro” deve ser avaliada em B6. As vantagens da utilização deste método de avaliação são:

- Proporcionar uma rápida avaliação da notícia e permitir uma compreensão universal.
- Ao longo de um determinado período de tempo, dar uma indicação das capacidades das várias origens e órgãos e ajudar a seleccionar as mais adequadas para determinadas tarefas.

0322. Análise e Integração

A análise e integração são definidas separadamente. A análise é um passo da fase de processamento do Ciclo da Produção da Informação que consiste em determinar e isolar os elementos significativos da notícia, para subsequente interpretação. A integração é um passo da fase de processamento do Ciclo da Produção da Informação que consiste na combinação dos elementos individualizados, obtidos por análise, com outras notícias ou informações já conhecidas, a fim de se formularem uma ou mais hipóteses lógicas. Na prática, os dois processos são tratados como um só, porque a análise é seguida pela integração, sem haver uma pausa entre ambas.

Na análise, procuram-se elementos significativos da informação registada e avaliada. Estes são então relacionados com outros já conhecidos e da comparação resultam deduções. A integração é a junção das deduções e a sua identificação com um padrão, com uma sequência de acontecimentos ou com uma imagem de um indivíduo. Este aspecto do processamento é essencialmente mental e é o ponto crítico no Ciclo da Produção da Informação, porque não existe ainda um substituto para a experiência e julgamento do analista.

Por isso, não existem regras ou indicações que se possam estabelecer para orientar ou auxiliar o analista na sua tarefa. No entanto, como é costume com outras tarefas que envolvem julgamento pessoal, a capacidade de interpretação do analista aumentará com a prática.

0323. Abordagem Multidisciplinar

De forma a evitar a decepção e a garantir a precisão da informação, devem ser utilizados, sempre que possível, meios de pesquisa de vários tipos. A informação deve ser processada a partir da informação obtida através do maior número possível de origens independentes, dentro do tempo e recursos disponíveis. A exceção deve ser a confiança numa única origem.

0324. Interpretação

A interpretação é o passo final da fase de processamento do Ciclo da Produção da Informação e consiste na determinação do significado de uma notícia relativamente a outras notícias ou informações já existentes. É onde a notícia registada, avaliada, analisada e integrada deve ser finalmente interpretada, para concluir o processo de conversão de notícia em informação.

0325. O Produto Final

O resultado do processamento resulta sempre num produto final (por exemplo: briefingue, análise ou relatório) que vai de encontro às necessidades de informação ou providencia uma mais-valia à condução das operações.

0326. O Processo Mental

A interpretação é o processo mental de comparação e dedução baseado no senso comum, experiência de vida, conhecimento militar sobre o inimigo e as forças amigas e as informações existentes. Nele, a nova notícia é comparada ou adicionada à existente, resultando em novas informações. Este processo mental pode ser dividido numa sequência de três questões principais, que devem ser levantadas sobre a notícia em consideração:

a. Identificação

Quem é? O que é? Isto não é apenas uma mera atribuição de identificação a uma unidade, ou um nome a um equipamento; é a consideração de todas as implicações da presença dessa unidade ou equipamento num determinado local, no tempo e no espaço.

b. Actividade

O que está a fazer? O significado do que está a fazer deve ser sempre comparado com a informação sobre a sua actividade anterior, para verificar se houve alteração no seu padrão de actividade.

c. Importância

O que significam as respostas às duas primeiras questões? Qual a sua importância? Têm alguma relevância para os indicadores de combate estabelecidos?

0327. Maximização do Uso da Informação

O analista deve ter a certeza que todas as possíveis deduções foram feitas a partir de determinada notícia. Uma forma de o fazer, é sempre que se faz uma dedução, perguntar a si mesmo “E então?” e quando responder a essa pergunta, questionar novamente “E então?”. Só quando não conseguir encontrar mais respostas, se pode concluir que foram extraídas todas as deduções ao facto.

0328. Decepção

A célula de informações é o alvo prioritário para a decepção. Por isso, o analista deve ser desconfiado por natureza, não deve tirar conclusões precipitadas e deve procurar confirmar, mesmo a mais credível das informações, da mais segura das origens. A história tem mostrado que a decepção pode ter grande sucesso e é uma componente poderosa e eficaz nas Operações de Informação.

0329. Confirmação

No fim do processo mental, as deduções e conclusões serão introduzidas no quadro de informações. No entanto, em quase todos os casos, a informação resultante não será conclusiva e haverá a necessidade de obter mais informação para confirmar ou rejeitá-la. A necessidade de preencher novos requisitos determina o carácter cíclico do Ciclo da Produção da Informação e a natureza repetitiva do plano de pesquisa.

0330. Considerações Finais

O tratamento sistemático da notícia e informações durante o registo, avaliação, análise, integração e interpretação é uma combinação de receber e arquivar a informação de uma forma ordenada e a aplicação lógica e metódica ao processo mental de converter notícias em informações. O processo mental, por si só, resulta de um conhecimento alargado das tácticas, equipamento e organização do inimigo, da elevada experiência do analista e da posse e aplicação de senso comum, aliado à capacidade para retirar deduções sensatas.

É a perícia do ser humano e a sua capacidade de “dar palpites” ou conduzir a análise de previsões baseadas em notícias incompletas que são fundamentais para o sucesso do processo analítico no centro do processamento. Essas perícias não são ensinadas, mas sim adquiridas e são o resultado da experiência e prática ao longo do tempo. São a chave da previsão natural das informações.

SECÇÃO V – DISSEMINAÇÃO**0331. Definição**

Disseminação é definida como a disponibilização oportuna de uma notícia ou informação, numa forma apropriada e através de meios adequados, àqueles que delas necessitam. Os seus principais componentes são:

a. Rapidez

Existem dois aspectos relativos à rapidez. O primeiro é que as informações que chegam ao destinatário demasiado tarde são inoportunas. O segundo é que a maioria das informações, aos níveis tático e operacional, são sensíveis ao tempo; isto é, o seu valor diminui ou desaparece com a passagem do tempo. Ambos os aspectos exigem que as informações sejam entregues aos seus destinatários tão rapidamente quanto possível. Quando o tempo para processamento é reduzido, as informações daí resultantes devem de ser anotadas para que o utilizador as trate com o adequado grau de discricção.

b. Adequação

Não é adequado disseminar informações que não respondam às necessidades do utilizador, que não sejam compreensíveis ou que sejam disseminadas por sistemas de transmissão que não estejam acessíveis ao receptor. As informações têm de ter um formato adequado às necessidades do receptor. Estas devem de ir ao encontro das suas necessidades, estar numa linguagem correcta e de serem disseminadas por um sistema comum a ambos, emissor e receptor. Caso contrário, serão inoportunas e sem qualquer valor. Assim sendo, deve ser estabelecida uma ligação entre o comandante e o seu estado-maior para garantir que as suas necessidades de informação são satisfeitas.

0332. Princípios da Disseminação

A disseminação é orientada pelos seguintes princípios:

a. Clareza

Deve ser sempre feita uma diferenciação clara entre factos e a sua interpretação. Em toda a documentação escrita, toda a interpretação deve ser precedida pela palavra “Comentário”. Numa apresentação oral, a diferença entre facto e interpretação deve ser sublinhada pelo uso de uma frase como “A conclusão a ser extraída disto é...” ou “Cremos que isto significa que...”

b. Concisão

Os comandantes não têm tempo para ouvir longas exposições orais ou ler extensos relatórios escritos. Os relatórios devem ser tão breves quanto possível; no entanto, devem incluir tudo o que se necessita saber. A eficácia das apresentações visuais na rápida partilha de informação deve estar sempre presente.

c. Normalização

Os relatórios podem ser compreendidos de uma forma mais rápida e fácil se forem escritos numa sequência lógica que sigam um formato normalizado. Existem publicações, tais como os STANAG, que contêm uma lista de relatórios de informações com os respectivos detalhes normalizados. Os formatos dos relatórios normalizados devem estar previstos nas Normas de Execução Permanente (NEP) (SOP - *Standing Operating Procedures*) da unidade.

d. Avaliação

Deve ser feita uma avaliação de cada parte da informação, incluída num relatório de informações, em vez de uma avaliação global do relatório. A avaliação deve ter o formato alfanumérico, já referido no parágrafo 322 deste capítulo.

e. Urgência

Sempre que possível, a notícia deve ser convertida em informações e disseminada, porque a interpretação dos factos é mais valiosa do que os factos por si só. No entanto, quando a rapidez é essencial, o processamento de notícia urgente pode não ser possível. Nestas circunstâncias, a notícia deve ser disseminada tão rapidamente quanto possível, com a limitação de não estar processada e poder não ser de confiança. Isto aplica-se particularmente a notícias e informações actuais, ao nível tático.

f. Distribuição

A célula de informações é responsável por assegurar que todas as notícias e informações sejam difundidas a todos os que delas necessitem, incluindo unidades adjacentes.

g. Regularidade

As notícias e informações urgentes, pesquisadas de acordo com as necessidades, são disseminadas sempre que estejam disponíveis. O comandante e a sua célula de informações necessitam, em complemento, de resumos de todas as informações que afectam as suas operações. Estes relatórios deverão ser incluídos nas NEP da unidade.

h. Segurança

As informações não devem ser sobreclassificadas, porque podem causar atrasos no seu manuseamento e na sua transmissão. Em regra, a informação respeitante ao inimigo não necessita de ser encriptada se o inimigo não tiver tempo suficiente para agir, caso intercepte a transmissão da informação. Por outro lado, deve ter-se cuidado para não revelar a origem da informação, havendo ocasiões onde o risco de comprometer a origem terá que ser ponderado face ao valor da informação, por forma a decidir se deve ser utilizada ou não. Nessas ocasiões, a célula de informações terá que recomendar qual o impacto de um possível comprometimento da origem, a fim de apoiar o comandante na tomada da decisão.

0333. Formatos de Disseminação

As notícias e informações podem ser disseminadas em quatro formatos: **verbalmente, por escrito, graficamente e como dados electrónicos.**

0334. Princípios da Disseminação Verbal

A exposição verbal é o método mais comum para a disseminação de notícias e informações. Deve ser orientada pelos seguintes princípios:

a. Clareza

Quem efectua uma exposição tem que assegurar-se de que seus pensamentos estão devidamente estruturados antes de a iniciar, devendo a mesma seguir um formato normalizado. Se necessário, o apresentador deve usar notas escritas para se assegurar que a sua exposição está de acordo com o formato. O uso de ajudas visuais, mapas, desenhos e diagramas auxiliam a exposição e clarificam a informação que está a ser apresentada.

b. Relevância

O apresentador deve assegurar-se de que as notícias e informações que estão a ser expostas são relevantes e actuais para as operações em que a audiência está envolvida; ou seja, que não estão desactualizadas ou que não tenham já sido apresentadas.

c. Brevidade

Ser breve e sucinto é a chave para o sucesso da disseminação de notícias e informações verbais. Um bom apresentador é aquele que transmite mais informação em poucas palavras.

0335. Tipos de Exposições Verbais

As exposições verbais podem ser:

a. De improviso

Acontece quando o comandante pretende ser actualizado com rapidez pela célula de informações. Isto, geralmente, acontece de uma forma informal e sem um formato rígido. Apenas incluirá os aspectos mais relevantes das informações que permitam actualizar o comandante relativamente ao último briefing.

b. Formal

É uma exposição preparada, destinada a um grupo constituído pelo comandante e o seu estado-maior ou comandantes de subunidades. Esta exposição exige algum tempo para a sua preparação adequada e deve ser feita de acordo com o formato normalizado.

0336. Canais de Comunicação

Para a disseminação verbal das informações, deve ser maximizado o uso de comunicações rádio e telefónicas, bem como comunicações de redes locais e de área. A escolha do sistema deve ter em consideração o estabelecimento da arquitectura das informações.

0337. As Vantagens e Inconvenientes da Exposição Verbal

As vantagens da exposição verbal são a sua rapidez, os factos serem expostos sucintamente e o orador poder ser questionado mais facilmente. As desvantagens são a dependência da personalidade do apresentador e a audiência quase sempre ter que se ausentar de seu local de trabalho, com as consequências que isso envolve. Isto pode ser ultrapassado se existirem meios de videoconferência (VTC - *Video Conferencing*) disponíveis.

0338. Princípios da Disseminação Escrita

Os princípios que se aplicam à disseminação verbal (clareza, relevância e brevidade) são igualmente aplicáveis ao processo de disseminação escrita.

0339. Documentos de Disseminação**a. Generalidades**

Os documentos com interesse para as informações, quer por a sua elaboração competir ao oficial de informações, quer por constituírem importantes meios na obtenção e disseminação de notícias e informações, agrupam-se em:

- estudos;
- anexo de informações;
- relatórios de informações.

b. Estudos

Compete à célula de informações a elaboração de diversos estudos, dos quais se destacam os seguintes:

(1) Estudo do Espaço de Batalha pelas Informações (IPB – *Intelligence Preparation of Battlespace*)

O IPB é um processo de análise da ameaça e do ambiente operacional, executado de uma forma sistemática e contínua, numa área geográfica específica que serve para apoiar o processo de decisão e os estudos do estado-maior.

A aplicação do processo do IPB ajuda o comandante a maximizar o uso do seu potencial de combate e a aplicá-lo no espaço de batalha de uma forma precisa, em pontos críticos determinados no tempo e no espaço, identificando a manobra mais provável (ou mais perigosa) por parte do inimigo e identificando os efeitos do ambiente operacional na sua unidade. Para além de ajudar o comandante no seu estudo de situação, o IPB constitui também um instrumento fundamental para a sincronização e produção dos planos de reconhecimento e de vigilância, da aquisição de objectivos, de pesquisa, de segurança das operações, de decepção, de contra-reconhecimento e outros.

O IPB é um processo contínuo e cíclico que se ajusta com as fases do estudo de situação de informações e que consiste em quatro passos principais:

- Passo 1 – Avaliação do ambiente no espaço de batalha;

PDE 2-00 Informações, Contra-Informação e Segurança

- Passo 2 – Descrição dos efeitos do espaço de batalha;
- Passo 3 – Avaliação do inimigo;
- Passo 4 – Determinação das modalidades de acção inimigas.

Os dados e informações que derivam de cada passo são representados graficamente numa série de transparentes que, quando sobrepostos permitem visualizar os aspectos relevantes das necessidades de informação.

O IPB é contínuo, iniciando-se antes da operação e tendo continuidade durante o seu desenrolar garantindo que os resultados continuem válidos e que se clarifiquem e apoiando o processo de decisão, ao mesmo tempo que dá indicações ao esforço de pesquisa, para a execução das operações correntes e a preparação das missões futuras.

De modo a facilitar o planeamento, a célula de informações prepara, se possível, o estudo de situação antes de os restantes elementos do estado-maior prepararem os seus estudos. O estudo de situação de informações constitui a base para os factos e hipóteses admitidos no processo de decisão, conduzindo os outros estudos e o processo de decisão. Os produtos do IPB são a base para o estudo de situação. Se o tempo disponível for curto para a produção de um estudo de situação escrito a célula de informações pode usar os produtos e resultados do IPB para as suas análises e avaliações.

(2) Estudo da Situação de Informações

Documento escrito que, tendo como elemento orientador a missão, analisa os aspectos mais característicos da área de operações e da situação do inimigo, com vista a deduzir a influência destes factores no cumprimento da missão e das modalidades de acção do inimigo e suas vulnerabilidades.

Difere do IPB por se tratar de um documento escrito, enquanto aquele é apresentado de forma gráfica.

c. Anexo de Informações

É um documento de disseminação de informações e transmissão de instruções relativas às actividades de informações visando uma determinada operação. Este documento constitui o processo formal de pôr em execução o plano de pesquisa³. É distribuído normalmente como anexo a um plano ou ordem de operações.

³ O plano de pesquisa é o documento que coordena os esforços dos órgãos de pesquisa à disposição de um determinado comando, e que, de acordo com as possibilidades de cada um daqueles órgãos, atribui missões de pesquisa. Trata-se de um documento de trabalho da célula de informações, que não constitui um apêndice ao anexo de informações e, como tal, não é difundido

d. Relatórios de Informações

As notícias e informações são disseminadas de forma escrita através de Relatórios de Informações. Estes são normalizados na Organização do Tratado do Atlântico Norte (OTAN) e estão descritos em STANAG (por exemplo, o STANAG 2511) que contém uma listagem de todos os relatórios de informações e detalhes sobre o seu preenchimento. Os relatórios podem ser de dois tipos:

(1) Relatórios Normais

Existem três relatórios de informações e que são os seguintes:

(a) Relatório Imediato (RELIM)

1. **Descrição:** O RELIM contém notícias ou informações de valor tático imediato, para as quais a velocidade de transmissão é de importância fundamental. Em regra, dizem respeito a um só assunto.
2. **Formato:** Não tem modelo prescrito; tanto quanto possível, deve responder às seguintes perguntas: QUEM? O QUÊ? QUANDO? ONDE? COMO? Um processo para não omitir estes aspectos é seguir a mnemónica «TUTELA», onde o T significa tamanho, U unidade, T tempo (GDH), E equipamento/armamento, L local (coordenadas) e A actividade.

(b) Relatório de Informações (INTREP – *Intelligence Report*)

O INTREP pode ter origem em qualquer escalão. Tem sempre que conter o título “INTREP” no cabeçalho das mensagens.

1. **Descrição:** O INTREP é um relatório difundido sem obediência a horários, sempre que as notícias ou informações disponíveis exigem a atenção do comandante destinatário. O INTREP deve conter algumas deduções derivadas das notícias e informações disponíveis na altura; as quais devem, em princípio, merecer a aprovação do comandante. A lista de distribuição normal deve estar estabelecida em NEP, em cada escalão de comando, mas isto não deve inibir o emissor do INTREP de alargar a distribuição se necessário.
2. **Formato:** O formato do INTREP deve estar de acordo com a normalização OTAN, podendo ser enviado em redacção livre. Para simplificar o processo, as mensagens contendo dados estruturados referentes a assuntos navais, terrestres ou aéreos foram desenvolvidos e com o formato base de MARINTREP, LANDINTREP ou AIRINTREP.

(c) **Sumário de Informações (INTSUM – *Intelligence Summary*)**

1. Descrição. O INTSUM é um relatório de informações conciso que contém, além das mais recentes notícias cujo processamento ainda não foi possível, um resumo das principais informações obtidas durante o período a que diz respeito, sobre a situação do inimigo, suas actividades e possibilidades e características da área de operações. O INTSUM é, normalmente, elaborado aos mais altos escalões. É um documento periódico, sendo a sua periodicidade fixada pelo comando imediatamente superior. É difundido para os comandos superior, subordinados e vizinhos, pelo meio mais rápido e adequado.
2. Formato: O formato do INTSUM deve estar de acordo com a normalização OTAN. Pode ser enviado em redacção livre. Existem alguns INTSUM que contêm informação específica sobre assuntos navais, terrestres ou aéreos e têm um formato específico. Estes designam-se por MARINTSUM, LANDINTSUM ou AIRINTSUM.

(d) **Relatório Suplementar de Informações (SUPINTREP - *Supplementary Intelligence Report*)**

1. Descrição: Este relatório pode ser elaborado a pedido ou na previsão de certas operações. Destina-se a coligir informações sobre um ou mais assuntos específicos com vista à preparação de uma determinada operação ou a recapitular todas as informações obtidas durante um período de tempo prolongado. Pode conter todas as informações disponíveis incluindo as já difundidas em INTREP e INTSUM. A sua distribuição é em função da natureza dos assuntos nele versados, sendo feita pelos meios mais adequados.
2. Formato: Não existe nenhum modelo normalizado para este relatório, a não ser a obrigatoriedade da palavra “SUPINTREP” aparecer no início de cada relatório.

(e) **Relatório Periódico de Informações (PERINTREP – *Periodic Intelligence Report*)**

1. Descrição. Documento de disseminação que contém elementos de informação relativos à situação e actividades do inimigo, às suas possibilidades e vulnerabilidades, às características da área de operações e às acções de contra-informação, sob a forma de um resumo ordenado de notícias pesquisadas e processadas durante um período superior ao do INTSUM. Não deve incluir qualquer referência

sobre as forças amigas ou assuntos de outra natureza que possam ter valor para o inimigo. É elaborado pelo Corpo de Exército e escalões superiores, sendo obrigatório a nível Exército.

2. Formato. Tem modelo prescrito. O período a abranger é fixado pelo comando imediatamente superior variando de acordo com o ritmo das actividades das informações, sendo que em combate, normalmente, é expedido de 24 em 24 horas.

(2) Relatórios Especialistas

Existem outros relatórios e sumários de informações que estão agrupados quer sob um determinado serviço, quer sob uma determinada especialidade.

0340. Disseminação Electrónica de Dados

Cada vez mais, as informações são disseminadas electronicamente. Isto exclui a necessidade de produção de mensagens escritas ou formatadas e tem a vantagem de permitir que as informações possam ser recebidas em tempo quase real, pelo seu receptor. Existe um grande número de aplicações de disseminação electrónica:

a. De Base de Dados para Base de Dados

A OTAN tem definido o formato comum ou estrutura em que as informações são disseminadas electronicamente. Se as bases de dados de informações estão de acordo com a estrutura OTAN, os dados não necessitam de ser alterados entre a extracção de uma base de dados e a sua transmissão e entre a recepção e o armazenamento na base de dados receptora. Neste caso, a velocidade e a facilidade da disseminação serão maiores. Se, por sua vez, a estrutura comum da base de dados for replicada em cada nível de comando, a disseminação de informações através da cadeia de comando será também simplificada e feita de maneira mais rápida.

b. Dados Não-Estruturados

As informações escritas, como relatórios de patrulhas, INTREP ou INTSUM podem ser armazenadas numa base de dados como texto. Além disso, os produtos de informações multimédia tais como imagens, vídeos, visualizações gráficas de situação e gráficos INTSUM podem também ser armazenados nas bases de dados.

0341. Comunicações

São necessárias comunicações robustas e redundantes para apoiar todos os aspectos operacionais do Ciclo da Produção da Informação. Para garantir a disponibilidade de comunicações adequadas, a célula de informações deve coordenar com a célula de Sistemas de Informação e Comunicações (CIS – *Communication and Information Systems*) para prever as necessidades de apoio em comunicações. Esta coordenação deve incluir a definição da arquitectura de informações, baseando-se nos requisitos dos sistemas, interfaces de interligação, largura de banda requerida e necessidades de segurança. No desenho da arquitectura de informações e na escolha dos sistemas a utilizar, devem ser tidos em conta os seguintes factores:

- a. **Velocidade.** A velocidade é essencial na disseminação das informações. Neste sentido, sempre que possível, deve ser utilizado um sistema de transmissões electrónico para transmitir informações em tempo quase real.
- b. **Encriptação.** A encriptação electrónica é instantânea e não tem nenhum efeito no tempo despendido na disseminação das informações. A encriptação manual consome muito tempo, devendo ter-se em conta que o processo de desencriptação no receptor do sistema de comunicações demorará algum tempo, provavelmente superior ao da encriptação. Se não houver nenhuma alternativa à encriptação manual e as informações forem urgentes, então o risco deve ser ponderado face à exigência de fornecer as informações ao utilizador em tempo oportuno.
- c. **Largura de Banda.** A largura de banda do sistema determinará a taxa em que as informações podem ser enviadas num sistema. Quanto mais estreita for a largura de banda, mais lenta será a taxa de transmissão. Esta consideração afectará a troca de grandes quantidades de dados, entre bases de dados, relativamente à disseminação de pequenas quantidades de informações. Se, contudo, a disseminação envolver gráficos tais como mapas, fotografias ou esboços, pode transformar-se numa preocupação, pois a sua transmissão é muito exigente em largura de banda.
- d. **Linguagem.** Se as informações são para ser disseminadas numa linguagem diferente daquela que é usada pelo receptor, uma situação que pode acontecer frequentemente nas operações combinadas, aliadas ou de coligação, deve considerar-se a utilização de um oficial de ligação (LO – *Liaison Officier*) fluente na

linguagem do receptor. Este método de disseminação, embora lento, impedirá a possibilidade das informações serem mal interpretadas.

Página intencionalmente em branco

CAPÍTULO 4 PROCEDIMENTOS

SECÇÃO I – GESTÃO DA COORDENAÇÃO DA PESQUISA E DAS NECESSIDADES DE INFORMAÇÕES

0401. Metodologia

Logo que as CCIR e as PIR tenham sido identificadas, pode iniciar-se o processo de planeamento de pesquisa de notícias e informações necessárias para lhes dar resposta. A metodologia que foi desenvolvida para elaborar o Plano de Pesquisa e para gerir a sua conduta de forma mais eficaz é a CCIRM. A elaboração de um Plano de Pesquisa eficaz, de acordo com os princípios das informações, é a chave para obter as respostas às CCIR e PIR.

A CCIRM abrange as actividades que resultam numa efectiva e eficiente aplicação das fases do ciclo da produção da informação, para satisfazer necessidades de todos os níveis de informações. É uma função de gestão que possibilita o fluxo temporal de informações, ao coordenar os esforços de pesquisa de notícias com o fornecimento das mesmas. A CCIRM consiste em duas componentes fundamentais:

- A coordenação da pesquisa;
- gestão das necessidades de informações que resultam de operações ou missões.

0402. Gestão da Pesquisa

A CCIRM é o processo de gestão da pesquisa e é definida como o processo de converter necessidades de informações em necessidades de pesquisa; estabelecer, atribuir ou coordenar acções com origens ou órgãos de pesquisa adequados; monitorizar resultados e reatribuir acções de acordo com as necessidades.

Apesar de o acrónimo CCIRM começar com a coordenação da pesquisa, seguido da gestão das necessidades de informações, a praticabilidade do ciclo da produção da informação demonstra que as necessidades precedem a pesquisa. As linhas gerais do conceito estão representadas na Figura 4-1.

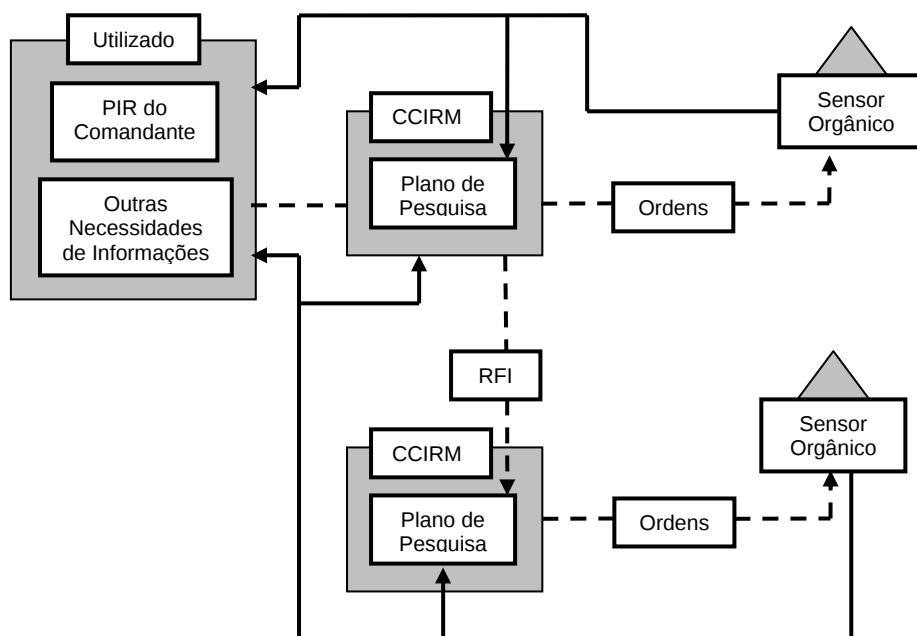


Figura 4-1 – Conceito CCIRM

0403. Gestão das Necessidades de Informações

A Gestão das Necessidades de Informações (IRM – *Intelligence Requirements Management*) inicia-se com a formulação das PIR do comandante que, uma vez identificadas, são apresentadas numa série de questões sob a forma de Necessidades de Informação (IR – *Information Requirements*). Os métodos seguidos para responder a estas questões formam a base de um Plano de Pesquisa. O papel da CCIRM é:

- Gerir o Plano de Pesquisa, assegurando que não ocorre nenhuma duplicação desnecessária de ordens - apesar de haver ocasiões em que a duplicação (redundância) é deliberadamente planeada para obter uma confirmação da informação.
- Garantir que são utilizadas as origens mais adequadas para obter as notícias.
- Monitorizar as necessidades das operações em curso e orientar a distribuição dos recursos necessários para que essas necessidades sejam satisfeitas.

Normalmente, as IR são divididas em duas categorias: aquelas que derivam das necessidades de informações para as operações, que estão a decorrer e que requerem actualização regular, e aquelas que resultam de necessidades mais sensíveis, tais como PIR.

As IR serão reencaminhadas para a Secção de CCIRM adequada, acompanhadas de uma cópia que será distribuída numa rede de CCIRM mais abrangente. O pedido tem de incluir:

- Preferencialmente, uma ou mais questões concretas;
- O tipo de resposta requerido (se for conhecido);
- O tempo de validade da informação (LTIOV - Latest Time Information Of Value);
- Se a resposta é simples e única ou se é disponibilizada através de relatórios periódicos.

Após o registo de uma IR, as secções de CCIRM irão validá-la, clarificá-la e aperfeiçoá-la. Vão também proceder a uma avaliação de prioridades com a célula de operações para determinar a sua importância relativamente a outras operações e planos e por conseguinte a sua urgência em actuar, o que será baseado nas PIR do comandante. Se por qualquer razão uma IR for rejeitada, deverá informar-se quem a solicitou. Logo que este processo de validação inicial tenha sido concluído, a secção de CCIRM irá:

- Em primeira instância, providenciar uma procura em bases de dados ou publicações às quais tenha acesso, de forma a garantir que a resposta não existe noutros registos. A secção de CCIRM irá, então, determinar se tem capacidade para responder aos pedidos, ficando responsável pelo seu processamento ou, caso contrário, o pedido será feito através da cadeia de comando, sob forma de um Pedido de Pesquisa (RFI – Request for Information), até que as secções de CCIRM, a um escalão mais elevado, possam satisfazê-lo.
- Se tiver capacidade para satisfazer as IR, as células de CCIRM identificarão e atribuirão Ordens de Pesquisa às origens ou órgãos que melhor possam fornecer a resposta.

0404. Coordenação da Pesquisa

A Coordenação da Pesquisa (CC - *Collection Coordination*) consiste na elaboração e controlo de um plano de pesquisa, o qual determina como é que as notícias e as informações necessárias para satisfazer as IR deverão ser pesquisadas. As IR são convertidas em ordens de pesquisa, constituídas por questões específicas colocadas às origens e aos órgãos orgânicos ou, caso não existam ou não sejam adequados, são convertidas em RFI. O RFI é a forma na qual uma IR é comunicada às entidades de CCIRM, a escalões superiores, subordinados ou adjacentes. O plano de pesquisa é permanentemente revisto e actualizado, devendo as células de informações

PDE 2-00 Informações, Contra-Informação e Segurança

supervisionar a produtividade das origens e órgãos, à medida que estes vão executando o plano de pesquisa. A Coordenação da Pesquisa tem duas partes:

- A exploração das origens pelos órgãos de pesquisa.
- A entrega de notícias obtidas à unidade de processamento adequada, para a produção de informações.

Depois de uma ordem de pesquisa ter sido concluída, as respostas são directamente enviadas a quem as solicitou. Este poderá ser um escalão superior, subordinado ou adjacente à unidade que a processou. O único envolvimento da secção de CCIRM será o de interlocutor entre quem processou a notícia e quem a solicitou, tendo sempre presente a LTIOV para confirmar que o envio foi ou será cumprido. Se houver dúvida quanto ao facto de se poder cumprir em tempo, a secção de CCIRM consultará a entidade requerente para averiguar se é aceitável fornecer a informação mais tarde ou se a ordem deve ser cancelada, libertando os meios para outras actividades. Se a resposta ao pedido não chegar a quem o solicitou, dentro da LTIOV, a secção de CCIRM apropriada deverá ser alertada.

0405. Procedimentos da Secção de CCIRM

O conceito de CCIRM é baseado nos princípios das informações. Inclui tanto a Coordenação da Pesquisa como a Gestão das Necessidades de Informação e o seu principal objectivo reside no fornecimento atempado da melhor informação possível.

As secções CCIRM desenvolvem as seguintes acções:

- Elaborar e gerir o plano de pesquisa.
- Converter as IR em ordens de pesquisa ou RFI.
- Fornecer respostas às IR com os seus meios orgânicos, sempre que seja possível.
- Enviar RFI, através da cadeia de comando, de modo a obter notícias que não estejam disponíveis ao seu escalão.

As secções de CCIRM nos mais altos escalões conduzem as seguintes acções:

- Validar e priorizar os IR.
- Registar os RFI e actualizar o Plano de Pesquisa.
- Responder aos RFI dentro das suas possibilidades.
- Converter os pedidos em ordens de pesquisa às origens e aos órgãos que estejam sob a sua autoridade. Estes deverão reportar directamente a quem as solicitou e

informar as secções de CCIRM que estejam responsáveis pela atribuição das ordens.

SECÇÃO II – OPERAÇÕES DE INFORMAÇÃO

0406. Generalidades

As INFO OPS definem-se como as acções coordenadas que visam influenciar os decisores e o processo de decisão do inimigo ou terceiros⁴, em apoio dos nossos objectivos políticos e militares, afectando os seus sistemas de comando e controlo (C2) e os seus sistemas de informação e comunicações (SIC) (CIS - *Communications and Information Systems*), ao mesmo tempo que exploram/protegem os nossos sistemas C2 e SIC. Existem duas categorias principais de INFO OPS, dependentes da natureza das acções desenvolvidas: INFO OPS ofensivas e INFO OPS defensivas.

Desde o nível estratégico até ao tático, as actividades das INFO OPS não são actividades separadas para serem desenvolvidas de forma individualizada, mas são realizadas através da integração e sincronização de todos os elementos de poder nacional, incluindo as actividades militares. Ao nível operacional e tático, as INFO OPS permitem ao comandante ter a capacidade para moldar a percepção do comandante inimigo ou terceiro e, no limite, convencê-lo a evitar hostilidades.

Genericamente, as INFO OPS têm como objectivos:

- atacar a percepção que o comandante inimigo ou terceiros têm sobre a situação, enfraquecendo a sua vontade e intenções e criando-lhes uma percepção da inevitabilidade de derrota, enquanto lhes oferecem opções alternativas plausíveis para a sua acção;
- persuadir o comandante inimigo ou terceiros a pensar aquilo que queremos, fazendo-os tomar as opções que nós queremos que eles tomem.

As INFO OPS afectam a capacidade de comando do inimigo ou terceiros, paralisando-os e impedindo-os de tomar iniciativas. Ao mesmo tempo, protegem a nossa coesão, mantendo a integridade dos nossos sistemas Comando e Controlo (C2) e SIC.

0407. O Ambiente da Informação

As INFO OPS são conduzidas num ambiente de informação que é um encadeamento de indivíduos, de organizações e de sistemas que pesquisam, processam ou

⁴ Estes últimos, desde que tenha havido aprovação política ao mais alto nível.

PDE 2-00 Informações, Contra-Informação e Segurança

disseminam informação, assim como a informação propriamente dita. O ambiente de informação é uma das componentes do espaço de batalha, que inclui:

- a internet;
- os sistemas C2 de forças amigas e inimigas;
- todas as entidades que tomam decisões e lidam com a informação;
- o terreno, as condições meteorológicas e os efeitos das armas que afectam o ambiente de informação.

Todas as operações militares são conduzidas dentro de um ambiente de informação, onde grande parte está para além do controlo militar imediato. De modo a conduzir operações com sucesso, o comandante terá de considerar a conduta das INFO OPS como uma parte integrante do ambiente de informação, que ele pode controlar, como parte do seu processo de tomada de decisão.

0408. A Conduta das Operações de Informação

O sucesso das INFO OPS colocará o inimigo ou terceiros em desvantagem ao explorar as suas vulnerabilidades e ajudará o comandante a alcançar e a manter a iniciativa e a contribuir para a FP. As INFO OPS moldam o espaço de batalha, permitindo ao comandante pensar, planear, comunicar e antecipar-se.

0409. Princípios de Operações de Informação

O planeamento e a condução de INFO OPS são orientados por uma série de princípios fundamentais que se aplicam de forma igual tanto às INFO OPS ofensivas como às defensivas:

a. Direcção e Envolvimento Pessoal do Comandante

As orientações do comandante reflectem as directivas dos escalões superiores e devem influenciar todo o planeamento dos seus escalões subordinados. A intenção do comandante define o esforço global das INFO OPS, especificando quais os objectivos para o plano das INFO OPS, contribuindo para apoiar a intenção estratégica e a missão. Desta forma, o comandante envolve-se pessoalmente na definição das orientações para as INFO OPS.

b. Coordenação e Sincronização

A própria natureza das INFO OPS e o alargado e diverso leque de efeitos sobre o alvo significam que tem de haver uma integração estreita dentro do comando.

Todos os planos e actividades de INFO OPS têm de ser coordenados e sincronizados transversal e verticalmente através da cadeia de comando e com outras actividades militares, políticas e civis, de modo que uma actividade não comprometa, negue ou diminua o efeito desejado de outra. Esta é a principal responsabilidade do oficial de INFO OPS em nome do comandante.

c. Informações Precisas

Para o sucesso das INFO OPS é vital a existência de um bom apoio de informações sobre o ambiente operacional e acerca do actual ou potencial inimigo ou terceiros. O pessoal afecto às INFO OPS deve trabalhar em estreita ligação com a célula de informações para definir quais os requisitos de informações necessários para o planeamento, condução e avaliação da eficiência e eficácia das actividades de INFO OPS. O processo de JIPB é ampliado para apoiar as INFO OPS, incluindo a análise de factores humanos (cultura, religiões, idiomas, etc.), infra-estruturas, processos de tomada de decisões e vulnerabilidades nos SIC. Este JIPB serve de base para os estudos das INFO OPS.

d. Planeamento Centralizado e Execução Descentralizada

O princípio do planeamento centralizado e da execução descentralizada (dentro de linhas de operações definidas) aplica-se às INFO OPS a todos os níveis de comando. No entanto, o controlo centralizado pode ser necessário para certos tipos de actividades de informação específica, quando é exigido a todos os elementos da força envolvidos o cumprimento rigoroso de um determinado plano.

e. Escolha de Objectivos Baseada nos Efeitos

O espectro de objectivos das INFO OPS é vasto e inclui todo o processo da tomada de decisão e infra-estruturas de apoio (dados, sistemas de informação e principais decisores). Os efeitos poderão incluir a destruição, incapacidade, influência, negação de informação e decepção, e serão conseguidos através de meios letais e não letais. A escolha dos objectivos das INFO OPS começa com os efeitos desejados e só quando estes tiverem sido determinados é que é escolhido o método de ataque. Todo o planeamento para a escolha dos objectivos poderá influenciar e criar outros efeitos não intencionais, pelo que o pessoal afecto às INFO OPS tem de analisar essas consequências e tomar as acções adequadas.

f. Preparação Oportuna

O planeamento das INFO OPS tem de começar o mais cedo possível, particularmente quando a determinação das percepções é a chave para o sucesso, porque tanto o planeamento como a execução exigem tempo e os resultados podem demorar a surgir. Daí que a intenção e as directivas do comandante para as INFO OPS, como parte do processo de planeamento, têm de ser fornecidas o mais cedo possível.

g. Monitorização e Análise de Efeitos

O sucesso das INFO OPS reside na contínua monitorização e avaliação das suas actividades e efeitos de curto, médio e longo prazo. Isto é conseguido através da recolha de informações de todas as origens e de outros tipos de resultados obtidos nas actividades das INFO OPS.

0410. Apoio das Informações às INFO OPS

As IR para as INFO OPS são muito amplas e variadas. As CCIR e as PIR para as INFO OPS são desenvolvidas usando a mesma metodologia que a usada para operações convencionais, mas as origens e as estruturas utilizadas são frequentemente mais vastas do que o ISTAR convencional. A Informação de Fonte Aberta (OSINT – *Open Source Intelligence*) é bastante viável, tal como a HUMINT, para identificar reacções humanas e, mais importante que isso, as suas percepções. As notícias e informações podem ser recolhidas num campo muito mais vasto. Por exemplo, a identificação de percepções numa Área de Operações Conjunta (JOA – *Joint Operational Area*) pode ser obtida através de comunidades de emigrantes que vivem noutros países. A análise terá também de considerar as implicações mais vastas de partes da informação e de relacioná-las com outros acontecimentos aparentemente sem relação entre si. As INFO OPS são de aplicação e resultados a longo prazo, devendo este facto ser tido em consideração pelas células de informações.

SECÇÃO III – O PROCESSO DE PLANEAMENTO OPERACIONAL**0411. Processo de Planeamento Operacional**

O OPP da OTAN é aplicável a qualquer QG estratégico, operacional ou tático. A célula de informações fornece dados fundamentais durante o decorrer do processo. Isto é acima de tudo derivado do JIPB, mas a informação também é produzida em resposta às

necessidades de informações que surgem no decurso da condução do OPP. No OPP existem ambos os processos e procedimentos. O processo global contém cinco fases.

a. Fase 1 – Iniciação

Uma sessão de planeamento pode ser iniciada a vários níveis. Esta fase começa com a recepção de uma Directiva Iniciadora ou Ordem Preparatória. Com base na directiva inicial, é criado um Grupo de Planeamento de Operações ou, caso já exista, é-lhe atribuída uma missão.

b. Fase 2 – Orientação

Uma vez recebida a Directiva Iniciadora ou Ordem Preparatória, o comandante irá determinar o que deverá ser cumprido. Isto é feito durante a Análise da Missão, pelo que haverá, nesta fase, o respectivo briefingue. O processo de Análise da Missão resulta numa Directiva de Planeamento do Comandante. Esta directiva detalhará vários aspectos tais como: pressupostos, centros de gravidade, tarefas, objectivos, estado final desejado e critérios para o sucesso. A fase 2 está demonstrada na Figura 4-2.

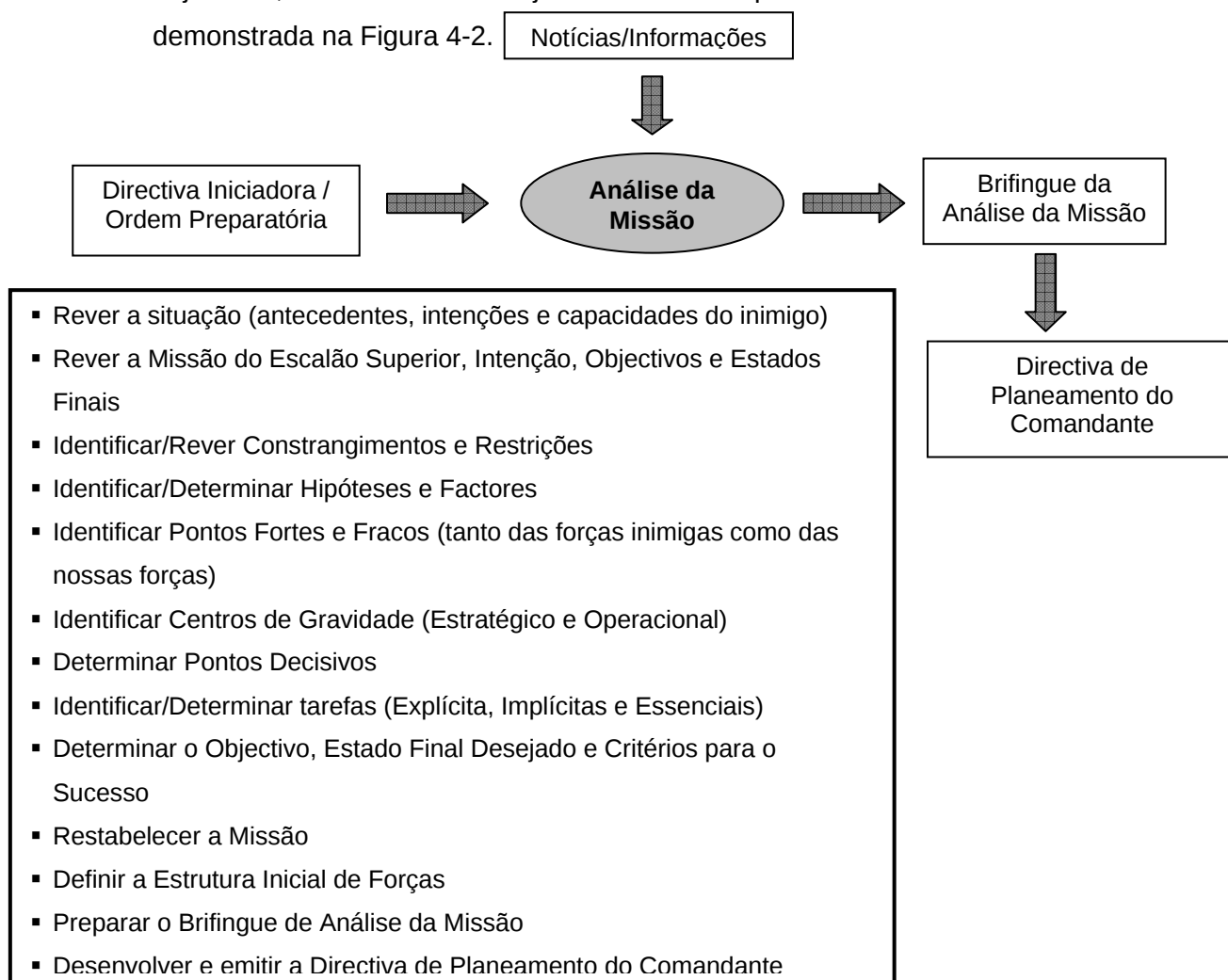
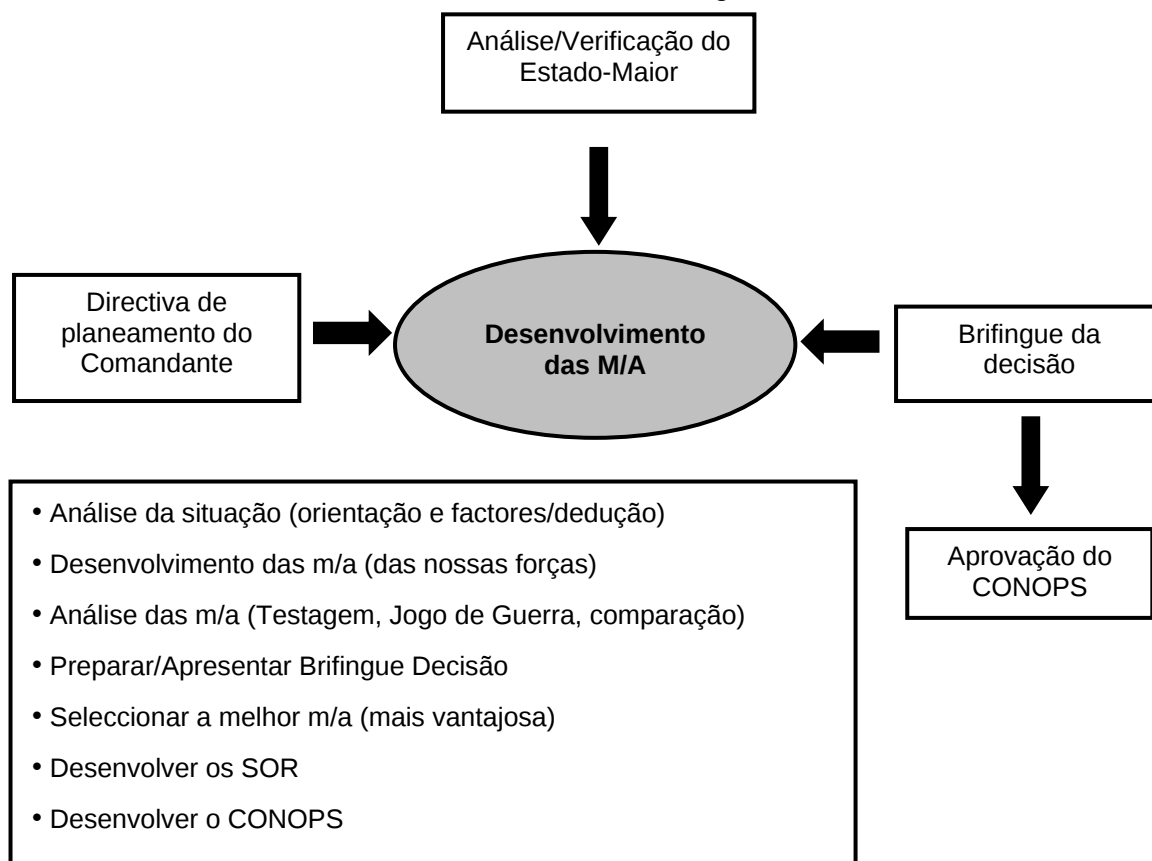


Figura 4-2 – Orientação

a. Fase 3 – Desenvolvimento do Conceito

A Directiva de Planeamento do Comandante é depois analisada e são desenvolvidas as modalidades de acção (m/a). As m/a são muitas vezes desenvolvidas usando a técnica de brainstorming, após o que é feito o Jogo da Guerra para determinar os Pontos de Decisão (DP – Decision Point). As m/a são desenvolvidas quer para forças amigas quer para as inimigas. Os resultados do jogo de guerra são apresentados ao comandante no Brifingue da Decisão. O comandante seleccionará a m/a a ser desenvolvida no Conceito de Operação (CONOPS – Concept of Operations) e a identificação dos requisitos e capacidades que as forças terão que possuir (SOR – Statement of Requirements) para executar o CONOPS. Esta fase está demonstrada na Figura 4-3.

**Figura 4-3 – Desenvolvimento do Conceito****c. Fase 4 – Desenvolvimento do Plano**

Nesta fase, o CONOPS é desenvolvido num plano, que é aprovado e posto em execução. Com base na complexidade das operações, as forças podem começar a ser utilizadas no fim desta fase. Esta fase está demonstrada na Figura 4-4.

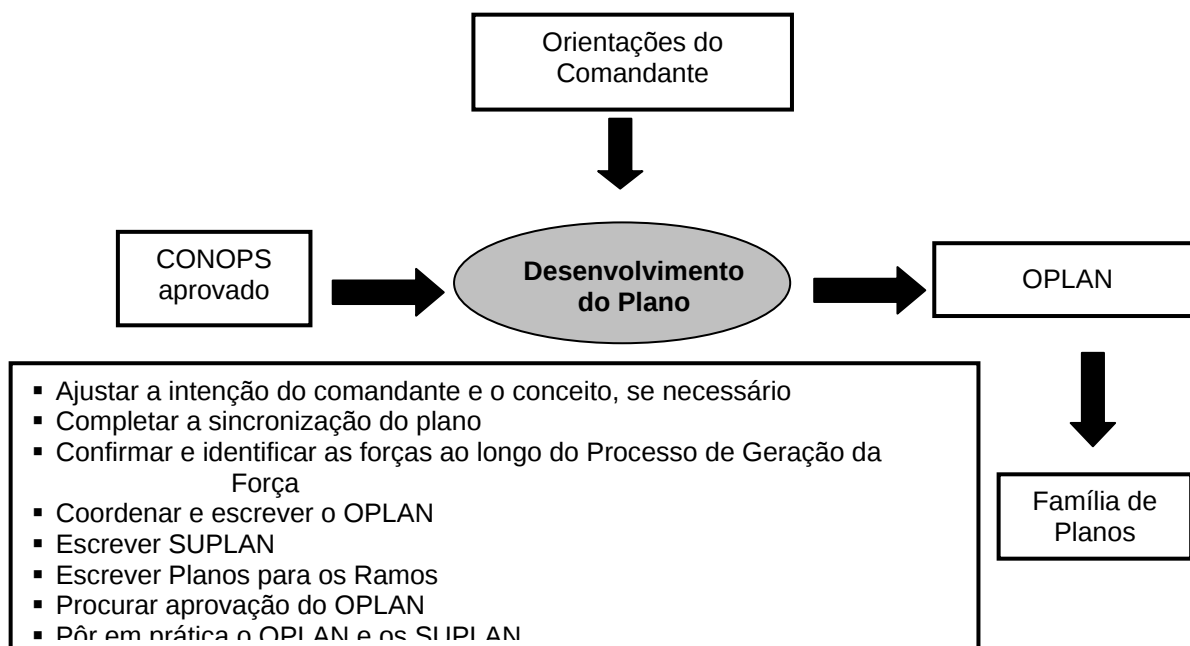


Figura 4-4 – Desenvolvimento do Plano

d. Fase 5 – Revisão do Plano

Esta fase contém dois passos – a Revisão do Plano e a Avaliação do Plano. Durante uma operação o plano é revisto à medida que esta decorre. Isto pode ser feito a pedido ou numa base periódica e previamente planeada. O plano é avaliado, normalmente, através do jogo da guerra ou outro critério. Se a avaliação determinar que são precisas mudanças significativas, pode ser efectuado outro brifingue da decisão. A fase de Revisão do Plano está demonstrada na Figura 4-5.

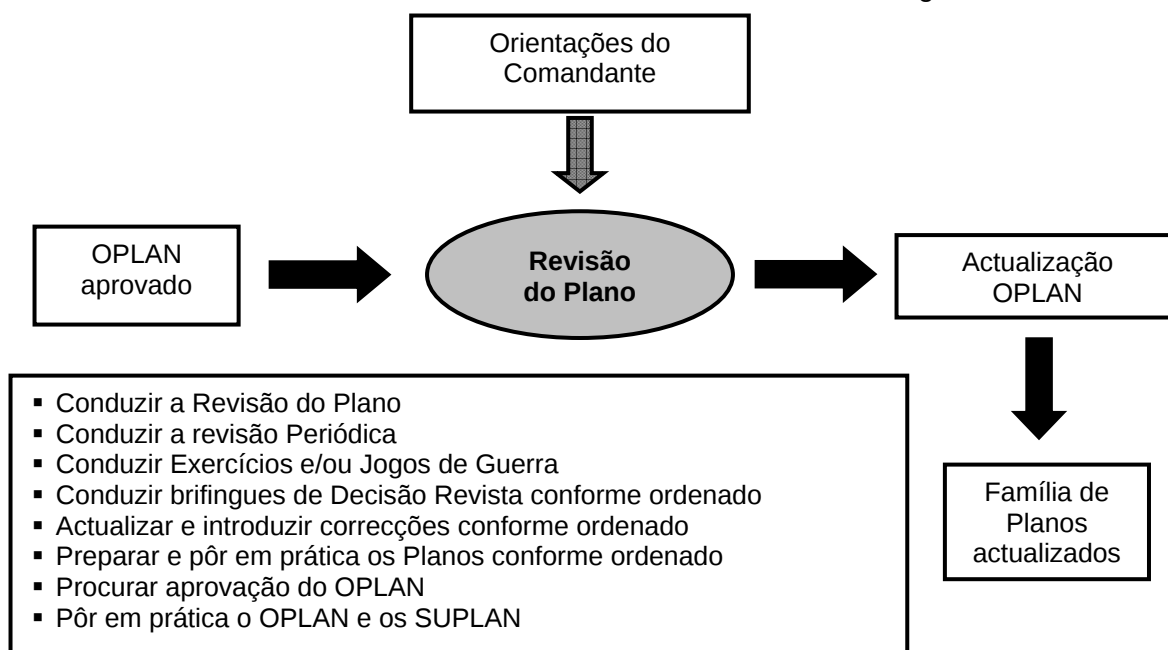


Figura 4-5 – Revisão do Plano

SECÇÃO IV – ESTUDO CONJUNTO DO ESPAÇO DE BATALHA PELAS
INFORMAÇÕES**0412. Generalidades**

O objectivo do JIPB é apoiar o processo de tomada de decisão do comandante, ao fornecer-lhe a base para obter uma Avaliação da Situação (SA – *Situational Awareness*)⁷. Permite, ainda, ao estado-maior responder às suas necessidades e orientar os elementos de reconhecimento e de vigilância para as actividades críticas.

O JIPB foi concebido para apresentar as notícias e as informações de forma gráfica, sendo apoiado mais facilmente pelas novas tecnologias de informação, do que se apresentadas de uma forma escrita. Os elementos básicos utilizados no JIPB são idênticos aos do Estudo da Situação de Informações (IE - *Intelligence Estimate*), sendo diferentes apenas os meios através dos quais esses elementos são desenvolvidos e apresentados. As principais vantagens do JIPB em relação ao Estudo da Situação de Informações incluem:

- a. Facilidade e rapidez em actualizar e apresentar uma elevada quantidade de notícias e de informações.
- b. Facilidade de assimilação de notícias e de proceder a correcções ao quadro de informações, face a alterações nos factores variáveis, à medida que elas ocorrem, através de simples alterações nos transparentes ou gráficos em computador.
- c. Facilidade de coordenação de grande quantidade, não prioritizada, de notícias que faça parte de bases de dados de informações.
- d. Facilidade em identificar áreas essenciais de interesse para as informações e pontos de decisão.

Apesar dos procedimentos aqui descritos serem primariamente aplicados a forças terrestres num espaço de batalha convencional, os princípios envolvidos também podem ser adaptados pelas outras componentes. Podem ser aplicados em qualquer ambiente operacional, designadamente selvas, montanhas, desertos, áreas urbanizadas, entre outras; e às funções de combate, tais como apoio de fogos, defesa aérea e guerra electrónica. O processo do JIPB também é apropriado às Operações de

⁷ O SA é a compreensão do ambiente operacional no contexto da missão do comandante

Resposta a Crises (CRO – *Crisis Response Operations*), incluindo as Operações de Apoio à Paz (PSO – *Peace Support Operations*). Em operações de contra-terrorismo, o processo do JIPB pode ser usado para se obter uma melhor compreensão das organizações inimigas envolvidas e das suas ligações internas e externas. Para além disso, as técnicas usadas no processo do JIPB podem também ser aplicadas à análise de operações de forças amigas, incluindo factores de mobilidade, meio envolvente do espaço de batalha e vulnerabilidades a acções de forças opositoras.

0413. Uso do Estudo Conjunto do Espaço de Batalha pelas Informações

Os princípios da JIPB podem ser aplicados em todos os teatros por forças terrestres, navais e aéreas e em todos os tipos de operações. O ponto até ao qual podem ser usados irá variar de acordo com as circunstâncias locais. Podem ser adaptados procedimentos precisos para ir ao encontro dos factores relevantes numa dada situação, da componente e da arma em causa, dos recursos do estado-maior e do nível do apoio tecnológico disponível.

0414. Conceito de Estudo Conjunto do Espaço de Batalha pelas Informações

O JIPB é um processo de informações sistemático, cíclico e dinâmico que está intimamente ligado às fases individuais do processo de tomada de decisão do comandante. Os resultados do processo do JIPB são representados graficamente numa série de transparentes. Os transparentes incluem elementos quanto ao terreno, às condições meteorológicas e à doutrina da ameaça, que podem ser preparados de forma antecipada. Imediatamente antes e durante o combate, os novos elementos disponibilizados serão adicionados e depois de integrados, demonstrarão graficamente o seguinte:

- a. Possíveis opções de ameaças.
- b. Locais onde os meios de pesquisa têm de ser colocados para monitorizar ou detectar ameaças.
- c. Locais onde as nossas forças podem influenciar o decurso dos acontecimentos, recorrendo às vantagens resultantes da manobra e acções ofensivas.

PDE 2-00 Informações, Contra-Informação e Segurança

- d. Os pontos de decisão nos quais o comandante tem de actuar para influenciar as operações da ameaça.

0415. Processo do Estudo Conjunto do Espaço de Batalha pelas Informações e o Ciclo da Produção da Informação

O JIPB está intimamente ligado ao Ciclo da Produção da Informação, dependendo das informações nele produzidas. Durante o processo do JIPB serão identificadas novas necessidades de informações, que serão então traduzidas em quesitos e as origens e os órgãos apropriados serão encarregues de proceder à pesquisa de notícias em sua resposta. Esses dados serão então processados, produzindo assim informações que são utilizadas nas várias etapas do processo do JIPB, na fase de planeamento e da conduta.

0416. Processo de Estudo Conjunto do Espaço de Batalha pelas Informações

O processo do JIPB consiste basicamente em três passos, apesar de algumas nações poderem dividir as várias tarefas em diferentes combinações, de forma a possuir mais do que três passos. Os passos são os seguintes:

a. Passo 1 – Avaliação da Área do Espaço de Batalha

Este passo avalia os efeitos de factores relevantes no que diz respeito ao meio envolvente do espaço de batalha, em operações conduzidas tanto por forças amigas, como inimigas. O seu objectivo primordial é identificar os Corredores de Mobilidade (CM) e Eixos de Aproximação (EAprox) da ameaça e das forças amigas. Em relação ao CT e à FP, incluirá o meio envolvente da ameaça no qual as forças militares e não militares operam; como por exemplo, a distribuição étnica da população e as suas lealdades. Alguns dos principais factores que afectam o meio envolvente do espaço de batalha são:

- (1) **Terreno.** Características tais como florestas, cursos de água, pântanos, terreno montanhoso, áreas urbanizadas, características hidrográficas e factores demográficos irão, aos vários níveis, restringir a capacidade de todas as partes para conduzir operações no espaço de batalha. Uma análise do terreno irá determinar as áreas de terreno livre, de terreno restrito ou de terreno impeditivo.
- (2) **Infra-estruturas.** A rede de comunicações que inclui elementos, tais como estradas, portos, praias e portos de abrigo, aeroportos, pontes e ligações ferroviárias é importante para a mobilidade e para a condução de operações.

Para além disso, em certos tipos de operações, poderá ser necessário limitar os danos a certas partes das infra-estruturas socio-económicas, tais como alojamentos, serviços públicos chave, instalações industriais e redes de transportes. A análise das infra-estruturas identificará objectivos que, pelas suas características, valor e/ou importância, tenham potencial para serem alvo de acções terroristas e que necessitarão, por isso, de protecção adicional.

- (3) **Ambiente de Informação.** As INFO OPS exigem uma análise detalhada do meio envolvente ao espaço de batalha, que inclui as características relevantes de nós de comando e controlo, redes de telecomunicações, notícias dos *media* civis e as atitudes e percepções dos decisores inimigos.
- (4) **Áreas Protegidas.** As leis dos conflitos armados determinam que certos edifícios e locais tais como monumentos, locais de culto, instalações médicas, etc., não devem ser usadas para fins militares ou ser atingidos. No entanto, o inimigo poderá utilizar estas áreas como bases de operações e isto será um factor a ser levado em conta ao determinar as necessidades de informação para a avaliação da ameaça à FP. A necessidade de evitar danos colaterais e baixas civis também colocará restrições às operações em centros populacionais importantes. Para além disso, algumas instalações, tais como centrais nucleares e instalações químicas poderão, caso sejam danificadas, constituir uma ameaça à segurança das forças amigas ou à população civil.
- (5) **Condições Meteorológicas.** As condições meteorológicas poderão influenciar a mobilidade. O mau tempo pode afectar de forma adversa as operações aéreas, marítimas e costeiras, assim como comunicações e a utilização de meios de vigilância e de aquisição de alvos. Períodos prolongados de tempo seco poderão permitir a passagem de pântanos ou atravessar obstáculos aquáticos. Num contexto mais lato, o clima determina a maneira como as operações são conduzidas, afectando o tipo de equipamento, apoio logístico e treino necessários para operações numa determinada área e meio envolvente.
- (6) **Factores Médicos.** A poluição do ambiente, doenças, efeitos de sistemas especiais de armas e outros riscos de saúde poderão afectar algumas ou todas as forças, assim como a população civil. As instalações médicas em nações anfitriãs, no teatro de operações, influenciarão o planeamento militar. As informações médicas serão essenciais para preparar avaliações de riscos de saúde, elaborar estudos de situação médicas e desenvolver regimes médicos preventivos.

- (7) **Outros Factores.** A composição étnica da população na área de operações e as atitudes das partes étnicas ou políticas, num dado conflito para com a presença das nossas forças na área, são um factor importante no planeamento e na execução de operações de apoio à paz.

b. Passo 2 – Avaliação da Ameaça

O objectivo deste passo é identificar as modalidades de acção da ameaça, independentemente dos constrangimentos impostos pelo terreno e condições meteorológicas; ou seja, saber como é que a ameaça vai actuar de acordo com a sua doutrina ou com base em anteriores experiências de combate. A avaliação da ameaça consiste em localizá-la, identificar a sua doutrina ou métodos de operação e determinar a sua modalidade de acção doutrinária. Em muitas operações de contra-terrorismo, onde a ameaça não actua segundo as regras doutrinárias, pode-se conseguir ajuda na dedução da modalidade de acção da ameaça através do estudo de operações anteriores de natureza semelhante. O resultado deste passo pode ser uma sobreposição de transparentes, ou uma série de sobreposições, que demonstram a disposição e a táctica para cada modalidade de acção doutrinária, como por exemplo a formação de ataque, o posicionamento das unidades em operações defensivas, etc.

Sobreposições demográficas adicionais e os alvos potenciais identificados durante a avaliação da área do espaço de batalha serão necessários para o CT e aspectos de FP de uma operação.

c. Passo 3 – Integração da Ameaça

No terceiro passo do processo do JIPB, os resultados do primeiro passo são combinados com as modalidades de acção doutrinárias e outros transparentes desenvolvidos no segundo passo. O objectivo deste passo é identificar como é que o meio envolvente do espaço de batalha irá determinar a doutrina e levá-la à prática. O processo deste passo consiste na produção de uma sequência de transparentes, como abaixo se indica:

- (1) **Transparente de Situação.** O modelo doutrinário da ameaça é moldado para se adaptar às restrições impostas pelos factores que determinam o meio envolvente do espaço de batalha; tais como o terreno, infra-estruturas, áreas protegidas, condições meteorológicas e outros factores relevantes. Com base na avaliação do objectivo, pontos fortes e fracos, possível colocação das forças

e tática da ameaça, é produzido um transparente para cada modalidade de acção, demonstrando o dispositivo tático adoptado ao longo dos CM e dos EApox identificados. O transparente deverá, ainda, incluir linhas de tempo demonstrando ritmos de progressão ou retirada e linhas de fase (PL – *Phase Lines*) indicando pontos no tempo e no espaço de importância crítica para o ímpeto da operação da ameaça.

- (2) **Transparente de Acontecimentos.** O transparente de acontecimentos deriva do transparente de situação e identifica graficamente quando e onde é que os acontecimentos chave poderão ocorrer. Locais onde possam ocorrer acontecimentos de importância para a condução da operação são designados por Áreas Designadas de Interesse (NAI – *Named Area of Interest*) e podem ser Pontuais ou de Área. A detecção e o reconhecimento de acontecimentos ou de actividades por parte da ameaça nesses pontos e áreas confirmarão ou negarão a intenção da ameaça em prosseguir com uma modalidade de acção específica. A identificação de NAI implica a atribuição de meios de pesquisa, através do Plano de Pesquisa, de modo a estabelecer e a manter a vigilância sobre essas áreas.
- (3) **Transparente de Apoio à Decisão.** O transparente de apoio à decisão é o produto final do processo de integração. É essencialmente uma informação conjunta e um estudo operacional em forma gráfica. As NAI identificadas no transparente de acontecimentos são aperfeiçoadas, pelos elementos afectos às informações e operações do estado-maior no decurso do jogo da guerra, para determinar Áreas de Objectivo de Interesse (TAI – *Target Area of Interest*). As TAI, que podem ser pontuais ou de área, são locais onde o comandante pode influenciar a operação ao destruir, retardar ou desorganizar a ameaça, utilizando os seus meios de ataque, como por exemplo reservas, artilharia e apoio aéreo. A identificação das TAI é o passo inicial para o processo de *targeting*. Tem de se identificar um DP ou uma Linha de Decisão (DL – *Decision Line*) por cada TAI. Os DP e as DL são pontos e linhas desfasados no tempo e no espaço em relação às respectivas TAI, em que o comandante tem de tomar uma decisão para usar os seus meios, se quiser influenciar a operação numa determinada TAI. Tal como com as NAI, é necessário manter a vigilância sobre as TAI e os DP, assim como a de adquirir dados sobre alvos futuros, que introduzirão novas necessidades no Plano de Pesquisa.

0417. Aplicação

Para além de possibilitar a um comandante a determinação das suas necessidades de informações através de uma apresentação clara e lógica, o JIPB também fornece a base para o jogo da guerra, que é utilizado para desenvolver o plano detalhado, ao confrontar as modalidades de acção determinadas pelo comandante ou pelo seu estado-maior com a modalidade de acção inimiga identificada como mais provável, através do processo do JIPB. O transparente de apoio à decisão, aperfeiçoado através do jogo da guerra, permite ao comandante e ao seu estado-maior um melhor acompanhamento da execução do plano.

Os produtos do processo do JIPB podem apoiar e ser melhorados pelo desenvolvimento de transparentes demonstrando, por exemplo, a avaliação da capacidade de fogos indirectos da ameaça, possíveis dispositivos da defesa aérea da ameaça, estudos da situação das capacidades de vigilância da ameaça, avaliações da capacidade de guerra electrónica e capacidade ofensiva nuclear, biológica e química.

0418. Estudo Conjunto do Espaço de Batalha pelas Informações e o Processo de Targeting

O processo de *targeting* está intimamente relacionado com o JIPB. Os dados iniciais de *targeting* são desenvolvidos a partir do primeiro passo do JIPB e aperfeiçoados nos passos subsequentes. As necessidades adicionais de informação surgem do processo de *targeting* e são integradas no Plano de Pesquisa.

Os resultados do JIPB e do jogo da guerra apoiam a identificação, selecção e localização, no tempo e no espaço, de Objectivos Remuneradores (HPT – *High-Payoff Targets*), que podem ser integrados no transparente de apoio à decisão como TAI. O JIPB também identifica os DP ou as DL em que o comandante tem de decidir usar os meios disponíveis contra uma determinada TAI. A necessidade de uma Avaliação dos Danos no Espaço de Batalha (BDA) exacta e atempada gera necessidades suplementares de informações.

SECÇÃO V – INFORMAÇÕES, VIGILÂNCIA, AQUISIÇÃO DE OBJECTIVOS E RECONHECIMENTO CONJUNTO

0419. Fundamentos

O ISTAR define-se como uma actividade de informações que integra e sincroniza o planeamento e o emprego de sensores e equipamentos e os sistemas de processamento, exploração, *targeting* e disseminação, em apoio directo a operações correntes e futuras⁶.

O ISTAR integra informações, vigilância, aquisição de objectivos e sistemas e sensores de reconhecimento, de forma a disponibilizar indicações sobre a manobra e os recursos para acções ofensivas, com particular ênfase na disponibilização atempada, quer de informação crítica, quer de *targeting*. Inclui a pesquisa, coordenação e gestão das notícias e das informações. A Avaliação da Situação (SA), obtida através das capacidades do ISTAR adaptadas, é fundamental para a tomada de decisão.

O objectivo do ISTAR, a todos os níveis, é produzir notícias e informações para ir ao encontro das CCIR, que resultam do OPP, e contribuir para a SA do comandante ao fornecer apoio a uma quantidade de funções, que incluem:

- OPP.
- Imagem Operacional Comum (COP – *Common Operational Picture*).
- *Targeting*.
- INFO OPS.
- FP.

O ISTAR é uma capacidade orientada por um comando aplicável a todas as operações. Parte integrante do ISTAR é a infra-estrutura do SIC, que interliga os componentes do ISTAR e permite a passagem atempada de informação para os comandantes e estados-maiores.

0420. Elementos

O ISTAR tem três elementos principais:

a. Notícias

Sob a forma de dados não editados ou já formatados.

b. Processos

O ISTAR integra continuamente o ciclo da produção da informação com partes do OPP e do ciclo de *targeting*.

c. A Arquitectura ISTAR

Inclui o conjunto de meios de pesquisa e a sua gestão, elementos de análise, utentes do produto e da infra-estrutura SIC que os liga entre si e a todos os níveis de comando.

0421. Actividades

O ISTAR tem quatro actividades primárias:

a. Informações

Ver parágrafo 106, Secção II, Capítulo 1.

b. Vigilância

A vigilância define-se como a observação sistemática do espaço aéreo, áreas superficiais ou sub-superficiais, lugares, pessoas ou coisas através de meios visuais, acústicos, electrónicos, fotográficos ou outros. A vigilância fornece e recebe indicações do reconhecimento e aquisição de objectivos para investigar actividades específicas ou para obter notícias mais detalhadas sobre uma determinada observação. A vigilância implica que o inimigo tenha de actuar ou movimentar-se, antes de ser detectado. Por natureza, a vigilância é passiva.

c. Aquisição de Objectivos

A aquisição de objectivos é definida como a detecção, identificação e localização de um objectivo, de forma suficientemente detalhada que permita o emprego efectivo de armas de fogos directos e indirectos. A aquisição de objectivos localiza forças adversárias com uma precisão suficiente, que permite atacá-las com sistemas de armas de fogos directos ou indirectos, proporcionando ainda outros efeitos com o emprego posterior de INFO OPS e da EW (emprego efectivo de sistemas letais e não-letais).

6 Definição funcional elaborada por acordo do Grupo "Joint ISTAR" da OTAN.

d. Reconhecimento

O reconhecimento é definido como uma missão destinada a obter notícias através da observação visual ou outros meios de detecção, relativas às actividades e recursos do inimigo, potencial ou não, bem como obter dados sobre as características meteorológicas, hidrográficas ou geográficas de uma determinada área. Geralmente, é um método orientado para obter uma notícia específica e que se caracteriza por uma duração temporal relativamente curta. O reconhecimento como actividade não está apenas limitado às unidades de reconhecimento, podendo também ser realizado por unidades não pertencentes ao sistema ISTAR, tais como observadores avançados de artilharia, forças especiais na retaguarda do inimigo, etc.

0422. Princípios e Considerações

O ISTAR partilha os princípios das informações; contudo há outras considerações a fazer. Os princípios e as considerações do ISTAR, quando correctamente aplicados, apoiam o OPP, contribuem para a SA e fornecem informação atempada sobre o objectivo. Estes são:

a. Orientações do Comando

A orientação do esforço do ISTAR e a determinação das prioridades devem ser definidas pelo comandante em cada nível de comando. Caso tal não se verifique, o comandante pode não obter as informações de que necessita para a tomada de decisão e conduta das operações.

b. Controlo Centralizado

O ISTAR deve ser controlado de forma centralizada, sem sacrifício do princípio da execução descentralizada implícita na missão do comando. Isto assegura, de acordo com as prioridades do comandante, o uso mais eficaz e eficiente de recursos limitados e, simultaneamente, a não existência de duplicações de esforços ou falhas na pesquisa.

c. Capacidade de Resposta e Oportunidade

O ISTAR tem de ser capaz de reagir às necessidades de notícias e de informações dos comandantes e de outros utilizadores, de uma forma oportuna. Isto permite trabalhar no âmbito do ciclo de acção-decisão do inimigo e contribuir para o ritmo

PDE 2-00 Informações, Contra-Informação e Segurança

operacional. A informação crítica tem de estar imediatamente disponível, ao nível em que é necessária.

d. Exactidão

As notícias têm de ser filtradas e analisadas para produzir informações precisas. As informações têm de reflectir o grau de confiança nas avaliações e nos julgamentos das informações. A série de acções a desencadear para manter o ritmo operacional funcionará contra esta exigência, sendo necessário um esforço significativo por parte do comando para balancear estas exigências e para assegurar que a exactidão não é sacrificada em detrimento da rapidez.

e. Combinação de Sensores

Uma integração eficaz das capacidades de diferentes sensores confere flexibilidade ao comandante para obter as notícias de que necessita. A combinação cruzada⁷ de sensores, melhora a eficiência ao reduzir a área de busca, o processamento e o ritmo operacional. Os meios ISTAR devem ser modulares, de modo a que se adaptem às necessidades da missão e do tipo de conflito.

f. Protecção da Fonte

Os meios de pesquisa têm de ser adequadamente protegidos durante a recolha de notícias. Haverá sempre um elemento de risco físico, político ou militar na utilização de um determinado conjunto de meios de pesquisa. Tem de se conseguir um equilíbrio entre o risco de perda de meios e as notícias e informações a obter. Do mesmo modo, o recurso a um conjunto de meios poderá indicar ao inimigo o que está a ser pesquisado e que, por sua vez, poderá fornecer indicações sobre os planos das forças amigas.

g. Interligação

Para dotar os comandantes e os estados-maiores, aos vários níveis, de uma melhor avaliação de situação, é necessária uma rede flexível, integrada e acessível de dados pesquisados, processos de informações, sistemas de armas e bases de dados. Esta rede deverá fornecer os meios para aceder às notícias e às

⁷ A combinação utiliza dados de um sensor para apontar ou colocar outro sensor a fim de obter dados adicionais que poderão melhorar ou clarificar um detalhe específico.

informações a partir de outros sistemas de pesquisa, órgãos e origens nacionais e multinacionais, de modo a satisfazer as necessidades de notícias e de informações do comandante.

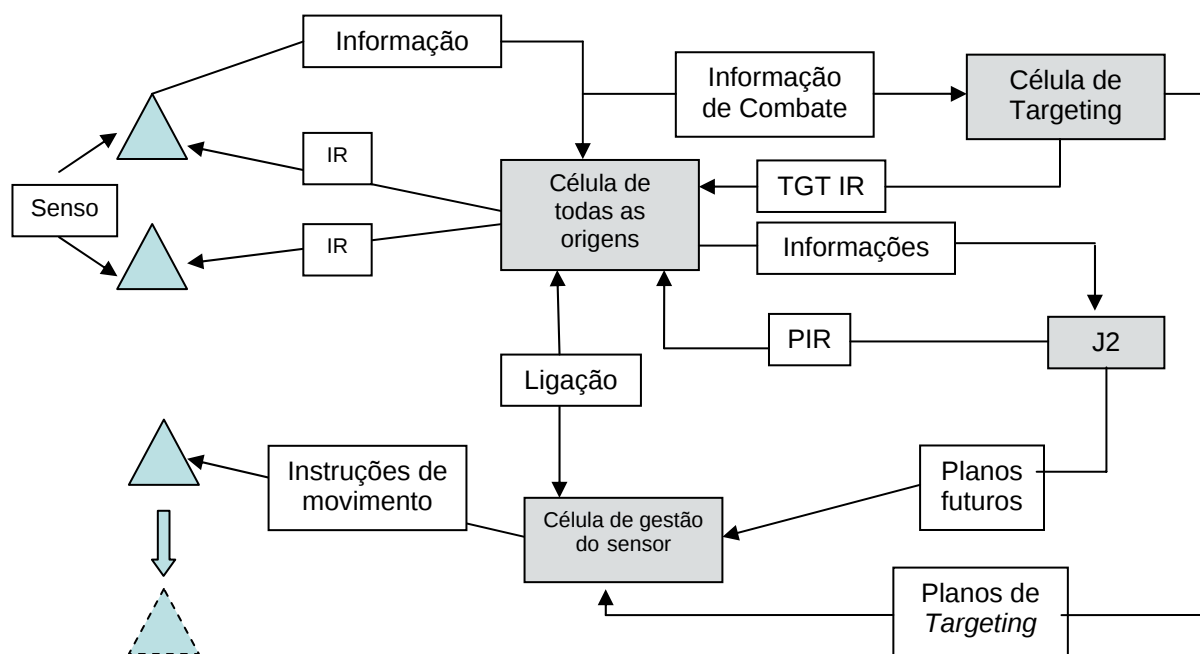


Figura 4-6 – Fluxo da informação e das informações no ISTAR

0423. Apoio ao Planeamento Operacional

O OPP inicial para responder a crises emergentes é baseado em informações estratégicas, correntes e básicas, e nas avaliações ao nível estratégico. As notícias e informações necessárias para este planeamento são pesquisadas, processadas e disseminadas em tempo de paz pelos recursos estratégicos nacionais.

0424. A Imagem Operacional Comum

A COP é uma imagem permanentemente actualizada do espaço de batalha. A COP reflecte as notícias acerca das próprias forças (imagem azul), forças inimigas (imagem vermelha), forças neutras (imagem branca ou verde), meio envolvente (imagem castanha) e o estado dos meios de pesquisa do ISTAR. É formada pela resposta da base de dados de notícias e de informações que é transversalmente comum ao nível do comando e que está acessível ao longo desse nível de comando. A COP pode facilitar a gestão dos meios ISTAR ao fornecer ferramentas capazes de representar graficamente as localizações actuais e futuras dos meios, os respectivos sectores de pesquisa, os

PDE 2-00 Informações, Contra-Informação e Segurança

objectivos de pesquisa e os dados recolhidos, em tempo real. A visualização do ISTAR pode ser correlacionada em tempo real com a situação militar actual, facilitando assim a reprogramação dinâmica dos meios do ISTAR e outras tomadas de decisão temporalmente críticas.

0425. Apoio ao Targeting

O *targeting* é uma responsabilidade do comando e define-se como o processo de selecção de objectivos e determinação das respostas adequadas a efectuar nos mesmos, tendo em consideração os requisitos operacionais e as capacidades dos diversos sistemas. O ISTAR contribui para o *targeting* ao fornecer elementos de informação essenciais sobre alvos ou conjuntos de alvos que permitem o efeito a ser aplicado, assim como determinar o resultado do combate. O *targeting* exige uma acção coordenada entre as diferentes áreas de actividade do estado-maior. Isto é importante na medida em que os sensores e as capacidades de pesquisa, sob controlo e controlados por outros níveis de comando, têm de estar perfeitamente coordenados entre si para uma rápida e eficiente transmissão acerca de alvos momentâneos ou perigosos. O pessoal afecto ao ISTAR será sempre parte de qualquer equipa de *targeting* que venha a ser constituída. As principais áreas do *targeting* nas quais o ISTAR está envolvido são:

a. Aquisição de Objectivos

A aquisição de objectivos evoluiu de um simples apoio ao emprego de armas para o efeito pretendido face às características do objectivo. A aquisição de objectivos localiza forças inimigas com suficiente exactidão para permitir serem utilizados sistemas de fogo directo ou indirecto ou para permitir outros efeitos, tais como INFO OPS a ser utilizadas contra eles.

b. Desenvolvimento dos Objectivos

O ISTAR pode ser usado em alturas ou fases diferentes para preencher a necessidade de desenvolvimento dos objectivos. O comandante poderá, então, decidir que efeito pretende atingir e qual o método para atingir esse estado final.

c. Avaliação dos Danos no Espaço de Batalha

A BDA é a estimativa exacta e atempada dos danos resultantes da aplicação da força militar, quer seja letal ou não-letal, contra um objectivo⁸. A BDA pode ser

⁸ Definição funcional elaborada, de comum acordo, pelo Grupo "Joint ISTAR" da OTAN

aplicada seguindo o emprego de todos os sistemas de armas (aéreas, terrestres, navais e das forças especiais) através de toda a extensão de operações militares. Consiste na avaliação dos danos físicos, funcionais e no sistema de alvos. É a avaliação atempada e precisa dos efeitos da aplicação de força letal e não-letal contra um objectivo pré-determinado. Essa avaliação é uma responsabilidade primária da área das informações mas tem de estar estreitamente ligada ao processo de selecção de alvos e envolve uma estreita cooperação com as operações e o elemento de apoio de fogos do estado-maior.

0426. Apoio às Operações de Informações

As INFO OPS apoiam-se num conhecimento e compreensão detalhados do inimigo, da forma como ele toma decisões e como tanto ele como os seus sistemas processam as notícias. A análise dos factores psicológicos, políticos, culturais, comportamentais e outros factores humanos que influenciam a tomada da decisão, juntamente com uma análise detalhada das infra-estruturas e da capacidade militar, é decisiva para o sucesso. O ISTAR apoia esta análise ao fornecer uma quantidade coordenada de dados, notícias e informações sobre esses assuntos. O apoio do ISTAR é necessário para informar a conduta das INFO OPS, especificamente aquela que é necessária para o seu planeamento e desconflitualização e para o emprego de disciplinas militares disponíveis para atingir os efeitos das INFO OPS.

0427. Apoio à Protecção da Força

O ISTAR contribui para a FP ao fornecer informação sempre que necessário. As medidas para identificar e contrariar as ameaças são implementadas como resultado de um processo contínuo de avaliação das ameaças em conjugação com actividades de contra-informação e informações de segurança.

0428. Operações Multinacionais

O apoio das informações às operações multinacionais no seio da OTAN exige que o processo ISTAR seja conduzido em conformidade com os procedimentos acordados para a partilha de informação e para a coordenação e utilização dos meios de pesquisa do ISTAR. Durante as operações multinacionais, o produto das informações que apoia essa operação tem de ser partilhado, devendo existir ligações logo na fase inicial aos mais altos níveis da aliança ou coligação, de forma a assegurar que as operações de informações de cada participante são coordenadas. Esses procedimentos têm de estar

PDE 2-00 Informações, Contra-Informação e Segurança

previamente acordados e, idealmente, devem ser praticados antes de se dar início às operações multinacionais. É possível fazer duas partilhas, dependendo da natureza da operação multinacional e dos participantes:

a. Partilha Integrada de Informação

Nesta situação, os meios de pesquisa do ISTAR, os processos e o pessoal estão totalmente integrados. Isto permite o fluxo imediato de notícias e informações e uma sinergia no uso dos meios de pesquisa. Também reduz a duplicação e simplifica a difusão do produto em formatos que podem ser prontamente utilizados por elementos nacionais de forças diferentes. No entanto, a possibilidade de emitir informação nacional sensível poderá causar dificuldades para os participantes, que frequentemente serão apenas resolvidas através de pragmatismo aliado à compreensão das sensibilidades envolvidas.

b. Partilha Paralela da Informação

Nestas circunstâncias, as diferentes capacidades nacionais do ISTAR trabalharão de forma separada e muitas vezes paralela, com algumas ligações que permitem a troca de informação. Isto permite um controlo nacional da informação, da pesquisa e de assuntos de segurança, mas conduz à duplicação de esforços e poderá levar à suspeição quanto à quantidade de conhecimento não emitido pelos parceiros.

0429. Planeamento

O planeamento ISTAR coordena, integra e sincroniza o esforço de pesquisa dos equipamentos disponíveis. É contínuo e está interligado com o OPP e o processo de *targeting*. A orientação do ISTAR é baseada na determinação das IR. Estas derivam das CCIR e de outras necessidades que cobrem o espaço de batalha, forças inimigas, forças amigas e elementos neutros.

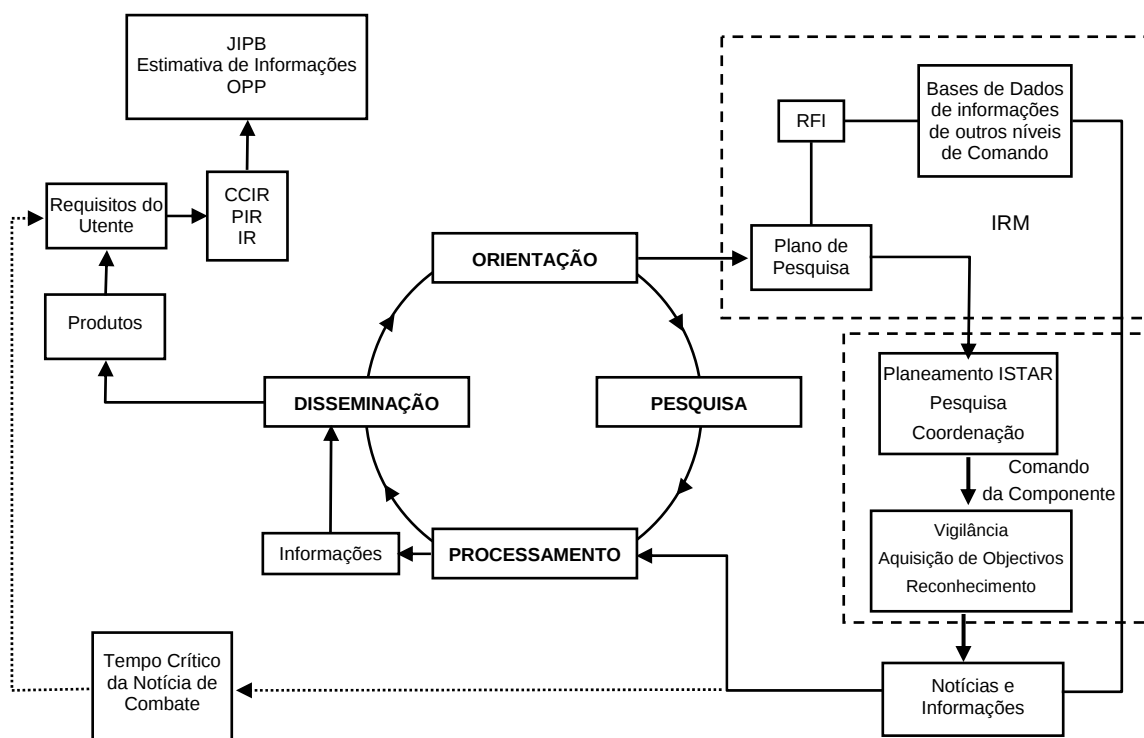


Figura 4-7 – O Processo ISTAR e o Ciclo da Produção da Informação

0430. Produtos do Planeamento ISTAR

O Processo de Planeamento ISTAR resultará em um ou mais dos seguintes produtos:

- Plano de Pesquisa.
- O Apêndice ISTAR ao Anexo de Informações à Ordem/Plano de Operações, que inclui o Transparente ISTAR e a Matriz de Sincronização ISTAR.

Juntos poderão ser referidos como o Plano ISTAR. O desenvolvimento de cada um destes produtos de planeamento ISTAR é explicado nos parágrafos seguintes.

0431. Plano de Pesquisa

O Plano de Pesquisa define-se como um plano para a recolha de notícias de todas as origens disponíveis, a fim de satisfazer as necessidades de informações e transformá-las em ordens e/ou pedidos aos órgãos de pesquisa apropriados. O desenvolvimento do Plano de Pesquisa é responsabilidade da célula de informações do estado-maior, em coordenação com os restantes elementos do estado-maior. Não é um produto específico das informações, mas um produto integrado de estado-maior. O Plano de Pesquisa estabelece a orientação para o esforço de pesquisa, a fim de satisfazer as necessidades do comandante, do processo do JIPB e da entidade responsável pelo

PDE 2-00 Informações, Contra-Informação e Segurança

targeting. Irá conter as necessidades detalhadas de notícias, as origens e os órgãos de pesquisa que estão disponíveis, bem como outros detalhes tais como janelas temporais relevantes para a pesquisa.

0432. Apêndice ISTAR

O Apêndice ISTAR pode consistir no Transparente ISTAR e na Matriz de Sincronização ISTAR. O Transparente ISTAR é uma representação gráfica do Plano de Pesquisa. Atribui a responsabilidade pela observação dos NAI (parte do JIPB), processo de pesquisa ISTAR e unidades. Isto é estabelecido de acordo com a disponibilidade de meios e das tarefas que lhes são atribuídas no Plano ISTAR.

0433. Matriz de Sincronização ISTAR

A Matriz de Sincronização ISTAR é uma representação gráfica que liga o Plano de Pesquisa às necessidades de informações do comandante. A Matriz de Sincronização ISTAR é desenvolvida com base na distribuição prevista dos meios ISTAR e permite ao comandante e à célula de informações do estado-maior monitorizar os meios de pesquisa. A Matriz estabelece a execução do plano ISTAR, distribuindo os meios pelas tarefas, com janelas de tempo para a sua execução.

0434. Aperfeiçoamento do Plano

A célula de informações tem de monitorizar constantemente o plano ISTAR, como parte do princípio da revisão contínua, de modo a recomendar alterações ou um desenvolvimento adicional do plano. Com base no JIPB e nas CCIR, o estado-maior e a célula de informações identificam lacunas no esforço de pesquisa e desenvolvem um plano ISTAR baseado na disponibilidade de reconhecimento, vigilância e meios de aquisição de alvos.

0435. Parâmetros de Planeamento

A utilização dos meios de pesquisa ISTAR tem de ser cuidadosamente planeada, não sendo apenas uma função da célula de informações ou do processo ISTAR, mas sim algo que requer o envolvimento das diversas áreas do estado-maior e aos vários níveis de comando, para assegurar a consistência de esforços. A atribuição e a determinação dos meios ISTAR serão responsabilidade das células de informações e de operações. Os principais tipos de planeamento ISTAR são os seguintes:

a. Planeamento de Atribuição de Meios

Garante aos diversos níveis de comando os meios de pesquisa suficientes para satisfazer as necessidades de notícias e informações dos respectivos comandantes.

b. Planeamento do Emprego dos Meios Atribuídos

Destina-se a planear o emprego dos meios de pesquisa ISTAR atribuídos, de forma a garantir a informação necessária.

0436. Planeamento de Atribuição de Meios

A quantidade e os tipos de meios de pesquisa disponíveis irão variar em função da operação e de cada fase da operação, podendo ainda ser afectados por outras circunstâncias. Há que considerar os seguintes factores durante o processo de planeamento de atribuição:

a. Necessidades de Informação

Os meios ISTAR são atribuídos com base na necessidade global, determinada através da análise e da priorização das necessidades de informação validadas. A atribuição de meios ISTAR é otimizada através da identificação das necessidades de informação, pela análise destas e sua classificação por ordem de importância face às necessidades de outros comandos.

b. Redundância de Meios ISTAR

A articulação efectiva do ISTAR é necessária e deve consistir na integração de Imagens de Informação (IMINT – Imagery Intelligence) de superfície, sub-superfície, aerotransportada ou baseada no espaço, tripulada e não tripulada, bem como de meios de pesquisa de Informação de Transmissões Electromagnéticas e Comunicações (SIGINT – *Signals Intelligence*) e HUMINT, a cada nível de comando.

c. Tempo e Espaço

A natureza variável da guerra aumentou o espaço de batalha pelo qual cada entidade e unidade são responsáveis. Os meios ISTAR têm de ser atribuídos de modo a cobrir o máximo possível do espaço de batalha físico e electrónico, pelo

PDE 2-00 Informações, Contra-Informação e Segurança

maior período de tempo possível, enquanto permitem, adicionalmente, alguma redundância.

0437. Planeamento do Emprego dos Meios

Uma vez atribuídos, os meios serão empregues para apoiar o Plano ISTAR a cada nível de comando. No entanto, é importante tirar o máximo aproveitamento dos meios, muitas vezes limitados. O planeamento pode ser subdividido em três níveis:

a. Determinação dos Meios de Pesquisa Adequados

É o nível mais alto do planeamento, realizado sem grande detalhe e planeado de forma a adequar as capacidades de pesquisa existentes à especificidade de determinada necessidade de informação. Esta função é uma responsabilidade da célula de informações, com a colaboração de outros elementos do estado-maior.

b. Atribuição de Meios às Tarefas

Este é um nível de planeamento com maior detalhe, onde a utilização dos meios de pesquisa atribuídos é sincronizada com o plano operacional. A sincronização e a integração são levadas a cabo em cada nível de comando e entre os vários níveis de comando, para evitar duplicações desnecessárias.

c. Planeamento Tático

Esta é a aplicação prática das Tácticas, Técnicas e Procedimentos (TTP – *Tactics, Techniques and Procedures*) para a utilização dos meios de pesquisa. Inclui a combinação e a combinação cruzada. A combinação utiliza dados de um sensor para apontar ou colocar outro sensor a fim de obter dados adicionais que poderão melhorar ou clarificar um detalhe específico. Maximiza a utilização eficiente dos equipamentos ISTAR no apoio a múltiplas prioridades que, às vezes, também competem entre si. A combinação cruzada de sensores melhora a eficiência ao reduzir a área de busca e ao aperfeiçoar o processo de procura.

0438. Comando e Controlo

A coordenação eficiente do C2 é a chave para o sucesso do Processo ISTAR. A coordenação das necessidades de informação identificadas, com a atribuição e a aplicação dos meios de pesquisa e o processamento das notícias, origina uma sinergia

que permite a produção de informações exactas, de modo a que o utilizador as utilize de uma forma rápida.

Na OTAN, a organização e a natureza das estruturas necessárias num QG para conduzir o C2 do processo ISTAR, variam de nação para nação. Nos parágrafos seguintes são desenvolvidos as funções de C2 e processos, que ocorrem dentro do processo ISTAR, já que se estes forem normalizados, irão proporcionar a interoperabilidade que é uma parte integrante da conduta do ISTAR em operações multinacionais.

0439. Funções de Comando e Controlo

O C2 do ISTAR é implementado através do exercício de um variado número de funções. Ao descrever a função C2 deste modo, as nações têm a possibilidade de colocar no terreno organizações e estruturas que acham mais adequadas para satisfazer a necessária funcionalidade do C2. Por isso, a padronização está mais nos processos do que nas organizações que os conduzem. As componentes funcionais do ISTAR são:

a. O Comandante

O comandante assegura as orientações ao ISTAR através das suas CCIR.

b. A Célula de Operações

A função da célula de operações é:

- (1) Interpretar e aperfeiçoar as CCIR.
- (2) Actuar como utilizador do produto das informações resultante do processo ISTAR.
- (3) Coordenar a colocação e a atribuição dos meios de pesquisa orgânicos e dos que lhe forem atribuídos.

c. A Célula de Informações

Esta função compreende:

- (1) O Processo de Planos da Célula de Informações.
Neste, as CCIR são transformadas em PIR.
- (2) O Processo de Gestão das Necessidades de Informações.
Aqui, as PIR evoluem para IR.

PDE 2-00 Informações, Contra-Informação e Segurança

(3) O Processo das Origens

Este processo tem três sub-processos:

- (a) O processamento das notícias de todas as fontes.
- (b) A compilação da imagem vermelha que compõe a COP e a contribuição para as imagens castanha e branca.
- (c) A produção de informações ajustadas às necessidades.

0440. A Função de Coordenação de ISTAR

A coordenação do ISTAR poderá ser uma função conjunta das células de informações e de operações ou poderá ser uma função separada dentro do estado-maior. No processo de coordenação ISTAR:

- a. Os meios de pesquisa são atribuídos face às IR, através do Plano de Pesquisa.
- b. A coordenação ocorre entre os elementos do estado-maior de informações e de operações sobre a determinação dos meios/equipamentos de pesquisa.
- c. Os RFI são recebidos de outras unidades e adicionados ao Plano de Pesquisa.
- d. Os RFI são disponibilizados a outras unidades.

0441. A Função de Pesquisa

A função de pesquisa é composta por dois processos de pesquisa:

- a. O processo de pesquisa no qual a notícia é recolhida por elementos orgânicos da unidade.
- b. O processo de pesquisa no qual a notícia é recolhida por elementos que são atribuídos à unidade, articulados para essa acção, para uma determinada operação ou fase de uma operação.

0442. ISTAR e o Processo de Targeting

De modo a retirar o máximo de sinergias do sistema ISTAR, o processo de *targeting* deve, idealmente, ser totalmente integrado no processo ISTAR. É aceitável que os acordos nacionais possam não suportar esta integração, mas de modo a maximizar os

benefícios do ISTAR, deve-se manter a ligação mais estreita possível entre o processo de *targeting* e o restante do processo ISTAR.

0443. A Arquitectura ISTAR da OTAN

a. Características fundamentais

Uma arquitectura ISTAR tem as seguintes características fundamentais:

- (1) Permite ao comandante dirigir o esforço das informações.
- (2) Assegura que o estado-maior do ISTAR consegue gerir a pesquisa a todos os níveis.
- (3) Apoia a gestão das necessidades, a pesquisa coordenada, o processamento e a difusão a todos os níveis de comando.
- (4) Apoia a atribuição de meios de pesquisa, com base nas IR validadas.
- (5) Permite a troca de informação entre células de informações, bases de dados e meios de pesquisa, através de uma infra-estrutura SIC ⁹.
- (6) Apoia a passagem de informação nacional apropriada.

b. Arquitectura das Relações

A efectividade da arquitectura é baseada nas relações entre os elementos funcionais. Os elementos funcionais são:

- (1) Os comandantes e os estados-maiores que conduzem o processo ISTAR.
- (2) As unidades que detêm os meios de pesquisa.
- (3) Os próprios meios de pesquisa.
- (4) As SIC que permitem o processo.

c. Preparativos para a Partilha

As dificuldades podem surgir aquando da combinação para a partilha de informações entre as nações e quando os meios de pesquisa de uma nação são organizados por outra. A arquitectura ISTAR deve ser estruturada para facilitar o controle, a coordenação e a organização de meios multinacionais e o pedido e acesso à informação dentro das restrições nacionais.

⁹ Esta infra-estrutura é apoiada por uma efectiva gestão da informação.

d. Acordos de Troca de Informações

Já existem acordos abrangentes de troca de informações entre nações da OTAN. Estes acordos aplicam-se principalmente aos níveis estratégico e operacional, no entanto algumas medidas aplicar-se-ão ao nível tático. Estes acordos fornecem a base para a arquitectura OTAN ISTAR para cada operação. Uma vez que muitas das informações disponíveis à OTAN não lhe pertencem, mas são colocadas à sua disposição por nações membro, a OTAN não pode difundir automaticamente estas informações para estados não membros. Antes da colocação das forças, ou no momento mais próximo depois disso, têm de se definir, de forma clara e detalhada, as restrições a ser aplicadas. A arquitectura ISTAR para uma operação apenas OTAN ou mais abrangente inclui um número de restrições gerais, a seguir detalhadas. Um exemplo ilustrativo de uma arquitectura ISTAR está demonstrado na Figura 4-8.

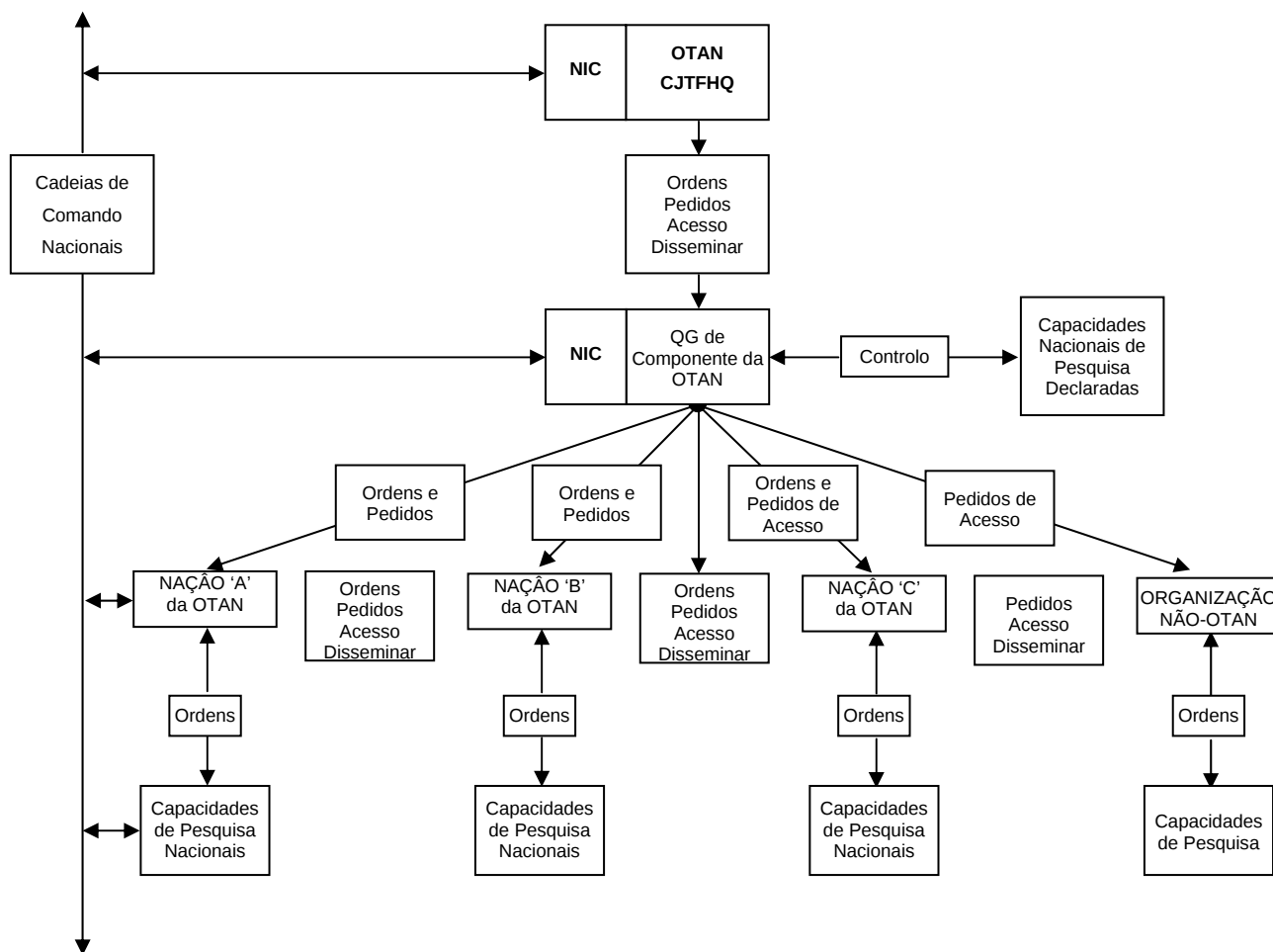


Figura 4-8 – Uma Arquitectura Genérica de ISTAR na OTAN

(1) Ordens de Pesquisa

Dentro de uma arquitectura ISTAR, a atribuição de pedidos de pesquisa a meios de pesquisa de outras nações OTAN só é possível dentro de alguns constrangimentos¹⁰, previamente acordados. Dentro de uma arquitectura ISTAR, a determinação de ordens de pesquisa mais abrangentes a nível multinacional por parte de nações não pertencentes à OTAN será a título excepcional, uma vez que os procedimentos habituais, tais como os que são implementados através dos STANAG, não são aplicados. A determinação de ordens de pesquisa não incluirá normalmente a capacidade para utilizar ou reutilizar os meios. Os meios nacionais declarados a um QG OTAN podem ser sujeitos à atribuição de ordens de pesquisa por esse QG. Qualquer meio que

¹⁰ Normalmente sob a forma de um Memorando de Entendimento (MoU – *Memorandum of Understanding*).

PDE 2-00 Informações, Contra-Informação e Segurança

seja declarado, mas controlado pela nação, pode ser sujeito à atribuição de ordens de pesquisa através dos procedimentos normais dessa nação. A prioridade que pode ser definida a tais tarefas deverá ter sido pré-determinada no início da operação. A atribuição de ordens de pesquisa a meios de pesquisa, que não tenham sido declarados pelas nações também é possível, mas à consideração da nação que os detêm.

(2) Pedidos de Pesquisa

A Arquitectura ISTAR apoiará os pedidos de qualquer nação a outra. As nações responderão a esses pedidos dentro da estrutura definida para essa operação. Isto será sempre discricionário, mas uma nação OTAN deverá legitimamente esperar que um pedido a outra nação OTAN seja satisfeito. Numa operação multinacional mais abrangente, a resposta estará ao critério da nação a quem é dirigido o pedido.

(3) Acesso e Disseminação

O acesso é a capacidade de conseguir aceder a notícias e informações. A disseminação é a passagem de produtos e avisos de notícias e informações a utentes específicos, sendo particularmente importante em relação ao que é temporalmente crítico. O acesso às notícias e informações deverá ser concedido sempre que o seja no quadro da Arquitectura, tanto a nível interno como externo em relação às unidades, enquanto que a difusão deve acontecer de forma natural e habitual. Dentro de uma operação OTAN deve de haver o mínimo de barreiras à capacidade de qualquer nação de aceder às notícias e informações onde quer que elas se encontrem, ou de a difundir a quem dela precise. Dentro de uma operação multinacional, serão aplicados controlos dinâmicos para assegurar que apenas as notícias e informações permitidas a nações não pertencentes à OTAN podem ser livremente acedidas e difundidas.

(4) Controlo

O controlo é a relação formal de comando entre o QG e os meios de pesquisa dentro de uma área de operações (AOO – *Area of Operations*). Este controlo será definido nos termos das normais relações de comando (OPCOM – *Operational Command*, OPCON – *Operational Control*, TACOM – *Tactical Command* e TACON – *Tactical Control*). O controlo implica, também, a capacidade de determinar tarefas, colocar e recolocar mais valias no terreno dentro da AO baseado na necessidade operacional.

0444. Contribuições Nacionais para a Arquitectura ISTAR OTAN

Cada nação que faça parte de uma operação multinacional irá colocar em terreno a sua própria arquitectura ISTAR. Essas arquitecturas nacionais deverão, ainda assim, funcionar dentro da arquitectura ISTAR OTAN. Há dois elementos específicos da arquitectura ISTAR própria de uma nação que podem ser colocados dentro da arquitectura ISTAR OTAN, que são:

a. Capacidades Nacionais de Pesquisa Declaradas

Em certas circunstâncias, as nações poderão fornecer capacidades de pesquisa próprias para uso da OTAN ou que podem ser definidas por outras nações. Se forem atribuídas a um QG OTAN, essas capacidades poderão estar sob uma relação formal de comando em relação a esse QG; caso contrário, continuam a ser controladas pela nação à qual pertencem. Estas capacidades declaradas incluirão sempre um elemento de comando que tem poder de veto (definido pela nação detentora) acerca da definição de tarefas. Esta é uma medida de controlo nacional para assegurar que um meio de pesquisa é usado de forma apropriada à operação e à postura da nação detentora.

b. Células Nacionais de Informações

As Células Nacionais de Informações (NIC – *National Intelligence Cells*) podem ser constituídas para operações OTAN. As NIC serão disponibilizadas por uma nação para assegurar o fornecimento de informações estratégicas nacionais à operação. Elas garantem a distribuição de informações às suas forças e, de forma adequada, ao pessoal das outras nações dentro da arquitectura ISTAR OTAN, baseada na política nacional de cada país. Podem também garantir a ligação entre uma nação e o QG colocado no terreno. A colocação no terreno de uma NIC é uma responsabilidade nacional, apesar do planeamento ter de considerar o seu apoio e os requisitos SIC. A sua localização dentro da arquitectura ISTAR será determinada por cada uma das nações.

SECÇÃO VI – O PROCESSO DE *TARGETING*¹¹**0445. Generalidades**

O processo de *targeting* é conduzido tanto em tempo de paz como de conflito. Em tempo de paz pode ser usado para apoiar o planeamento de contingência e o JIPB. As áreas de potencial colocação de forças no terreno podem ser “referenciadas” para recolha de informação. Em caso de crise ou guerra, o processo apoia o uso de armamento e dos meios de pesquisa de informações. O *targeting* não é apenas o processo de identificar um alvo geográfico: indivíduos, grupos, economias, assinaturas electrónicas e um vasto número de aspectos intangíveis podem todos ser referenciados para fins militares.

0446. O Processo

O processo de identificar potenciais objectivos é conduzido pela análise de informações sobre o inimigo, levando a propostas para que objectivos específicos sejam batidos. Esta análise é conduzida dentro do contexto dos sistemas ofensivos, ou outras capacidades à disposição do comandante, de modo a identificar vulnerabilidades específicas que, a serem exploradas, ajudarão a atingir a intenção do comandante e o estado final desejado. O *targeting* considera uma vasta área de actividades que não apenas a pura destruição por armas terrestres, aéreas e marítimas – inclui o uso de EW e outras técnicas de ataque não-letais. Como tal, é complementar a outras capacidades tais como as INFO OPS. O processo de *targeting* define quais os objectivos a serem batidos, com que meios e por que ordem de prioridades. Também especifica objectivos restritos ou que não podem ser batidos. Acima de tudo, o processo procura assegurar que todos os meios envolvidos saibam claramente quais os seus objectivos, quais as responsabilidades de coordenação e quais os constrangimentos de tempo e de espaço.

0447. Objectivos

Neste processo são considerados três grupos de objectivos:

a. Estratégicos

São os objectivos que, a longo prazo, afectem a capacidade e a vontade de um inimigo manter as hostilidades, como por exemplo, a capacidade C2 estratégico,

¹¹ A Doutrina OTAN Joint Targeting está em desenvolvimento. Esta publicação será corrigida de forma adequada quando a nova doutrina tiver sido aprovada.

infra-estruturas económicas, financiamento de terroristas ou objectivos que possam ter implicações para a população civil. Para além disso, todos os objectivos associados a armas de destruição maciça ou nucleares são classificadas como sendo de natureza estratégica.

b. Operacionais

São os objectivos que afectem a capacidade militar de um inimigo, como por exemplo sistemas de defesa aérea, armazenamento de munições ou depósitos de armamento terrorista, ou que apoiem directamente a capacidade inimiga de manter as hostilidades, como por exemplo linhas de comunicação ou bases seguras.

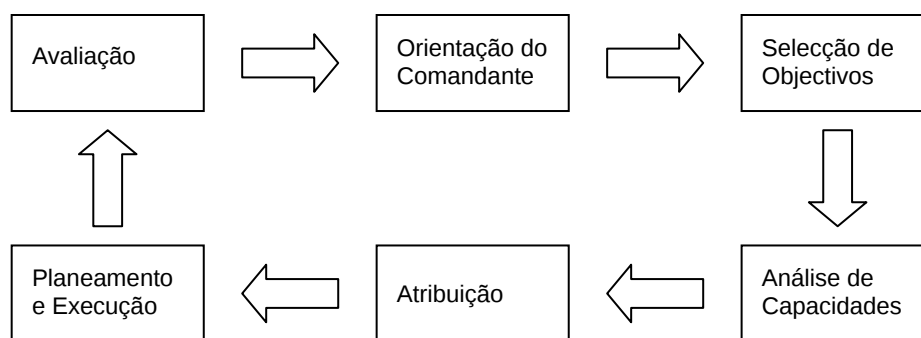
c. Tácticos

São as forças militares, regulares ou irregulares, de um inimigo que tenham o potencial para influenciar o espaço de batalha táctico do comandante.

As decisões de targeting tomadas aos níveis operacional e táctico podem apresentar resultados estratégicos. A tecnologia moderna, está permanentemente a aumentar o grau de eficiência com o qual as armas convencionais, e as armas não-letais, podem ser usadas para atingir objectivos estratégicos e operacionais. Manter o controlo sobre estas capacidades, para assegurar a sua aplicação de acordo com os objectivos nacionais, com os fins estratégicos e com o plano operacional da campanha, é importante e terá, inevitavelmente, implicações políticas. Por isso, a política e a direcção seguida no targeting são decisões tomadas aos níveis mais elevados. Quando as decisões de targeting são tomadas aos níveis operacional e táctico, têm de estar em conformidade com a direcção e o enquadramento estratégicos.

0448. O Ciclo de Targeting

A inter-relação das funções aplicadas na direcção da força militar contra um objectivo, é conhecida por Ciclo de *Targeting*. É o mecanismo através do qual os produtos do sistema ISTAR são inter-ligados aos meios ofensivos, de forma a assegurar que é utilizado o sistema de armas mais adequado, ou outra capacidade, para atacar cada objectivo. O *targeting* é um processo conduzido pela célula das operações, tendo por base as informações fornecidas pela célula de informações. Pode ser aplicado ao longo de todo o espectro de conflito e a todos os níveis de comando. É, no entanto, optimizado para bater objectivos em profundidade.

**Figura 4-9 – Ciclo de Targeting**

O *targeting* é conduzido de acordo com o Ciclo de *Targeting* demonstrado na Figura 4-9, sendo coordenado através da Célula de *Targeting* no QG Conjunto. A maior parte do processo de *targeting* é conduzida na fase de planeamento do OPP com muitas decisões de selecção de objectivos a ser tomadas antes do início da operação. Isto permite aos objectivos serem batidos assim que são identificados, não sendo necessária a intervenção do comandante.

A capacidade para controlar o Ciclo de *Targeting* de forma eficaz, ao mesmo tempo que se responde a mudanças de natureza operacional, é fundamental para a condução bem sucedida das operações. Os elementos chave na condução bem sucedida do processo de *targeting* são:

- a. A capacidade para detectar e avaliar potenciais objectivos;
- b. Pessoal treinado, incluindo a necessidade de todos os membros de uma Célula de *Targeting* multinacional serem treinados a um nível comum;
- c. Comunicações sólidas e gestão de dados;

A capacidade de providenciar uma SA¹² e BDA¹³.

¹² A Avaliação de Combate é composta por três componentes principais: BDA; Avaliação do Grau de Eficácia das Munições, Recomendação para voltar a bater o objectivo

0449. Passos

Os passos no Ciclo de *Targeting* consistem nas seguintes actividades:

a. Orientação do Comandante

A orientação e as prioridades operacionais emitidas pelo comandante;

b. Selecção de Objectivos

Este passo inclui a identificação de objectivos operacionais e táticos;

c. Análise de Capacidades

Neste passo, os alvos pretendidos são integrados numa Lista de Objectivos, ordenada por prioridades, para ser sujeita a aprovação, analisando-se as capacidades dos meios ao dispor do comandante.

d. Atribuição

É feita a correspondência de armas apropriadas, ou outras capacidades, aos respectivos objectivos.

e. Planeamento e Execução

É recolhida informação acerca de alvos individuais ou conjuntos de objectivos que, juntamente com informação dos meios disponíveis do comandante, vão sendo integradas no Plano de Execução. É neste passo que se determina qual/quais as componentes que irão bater os objectivos.

f. Avaliação

É feita uma avaliação dos resultados dos ataques ou de outras acções apropriadas sobre os objectivos e, conforme se julgue apropriado, são feitas recomendações no sentido de voltar a atacar determinado objectivo.

0450. Terminologia de Targeting

Há alguns termos básicos de *targeting* cuja compreensão é essencial para a condução do processo de *targeting*. Segue-se uma explicação desses termos:

¹³ Isto inclui BDA convencional e outras medidas de eficácia relacionadas com contra-terrorismo.

a. Lista de Objectivos Conjunta

A Lista de Objectivos Conjunta (JTL - *Joint Target List*) é a lista primária de objectivos para apoiar uma determinada operação. Representa os objectivos disponíveis para atingir efeitos estratégicos e operacionais que podem ser atacados na consecução dos objectivos operacionais.

b. Lista de Objectivos Conjunta, Integrada e Prioritizada

Após a JTL ter sido aumentada com os alvos retirados dos Planos de Operações das Componentes, obtém-se a Lista de Objectivos Conjunta e Integrada (JITL - *Joint Integrated Target List*). Esta, depois de aprovada, e de terem sido atribuídas prioridades, origina a Lista de Objectivos Conjunta, Integrada e Prioritizada (JIPTL - *Joint Integrated Prioritised Target List*). A JIPTL é a base para o processo de atribuição dos meios de ataque aos respectivos objectivos.

c. Objectivos Não-Restritos

São conjuntos de objectivos, tipos ou áreas, para os quais a aprovação para o ataque foi delegada ao comandante, sem necessidade de aprovação militar ou política superior. Permanecem sujeitos a validação legal.

d. Objectivos Restritos

Os Objectivos Restritos (RTL – *Restricted Target List*) são um subconjunto dos objectivos da JITL que requerem especial atenção, quando não se procura a simples destruição. Esta classificação poderá ser motivada pelos seguintes motivos:

- (1) Particular sensibilidade do local.
- (2) Pela necessidade de desconflitualizar qualquer acção proposta em relação a outras actividades.
- (3) A avaliação ao local determinou que tem demasiado valor para a pesquisa de informações.
- (4) Intenção de utilizar um único tipo de arma.
- (5) Intenção de explorar o objectivo.
- (6) Devido a considerações de reconstrução pós-conflito.

e. Lista de Objectivos Proibidos

É uma lista de objectivos a não atacar elaborada pelos elementos da Força Conjunta e aprovada pelo comandante. Esta lista também inclui objectivos, definidos por altas autoridades, para não serem atacados; e ainda outros alvos, cuja destruição poderá interferir ou pôr em causa operações militares projectadas, conduzidas por forças amigas, ou relações com a população ou governos locais. Aumentos ou cortes da Lista de Objectivos Proibidos (NSTL - *No-Strike Target List*) têm de ser cuidadosamente controladas e coordenadas pela Célula de *Targeting*, de forma a minimizar a possibilidade de fratricídio e para maximizar a eficácia do combate.

0451. Os Princípios Legais de Targeting

O *targeting* é conduzido de acordo com quatro princípios fundamentais:

a. Distinção

Os ataques são limitados aos combatentes e a outros objectivos militares.

b. Proporcionalidade

Isto exige que os objectivos militares não deverão ser atacados se o ataque puder causar baixas civis ou danos a objectos civis (baixas e danos colaterais) que seriam excessivos em relação à vantagem militar directa que se espera que o ataque produza.

c. Necessidade Militar

Qualquer acção militar tem de ser exigida pelas necessidades das operações militares e deve ser o mínimo exigido e não proibida pela Lei do Conflito Armado.

d. Humanidade

Este princípio proíbe qualquer ataque que provoque sofrimento, ferimentos ou destruição desnecessários a um inimigo, que possam ser justificados pela necessidade militar.

0452. Apoio das Informações ao Targeting

A resposta fornecida pela célula das informações nas várias fases do Ciclo de Targeting é determinante para o sucesso do Processo de *Targeting*. As ligações entre os passos no Ciclo de *Targeting* e o processo de informações estão esquematizadas a seguir:

a. Definição de Objectivos

- (1) A primeira fase nesta actividade envolve a identificação de objectivos chave. Os principais contributos para este passo do Ciclo, derivam dos TAI originados do JIPB e das Informações Básicas incluídas em bases de dados de informações nos níveis estratégico e operacional de comando.
- (2) Após a identificação destes objectivos chave, procede-se à sua análise de forma a determinar os tipos de objectivos aos quais o esforço (ME - *Main Effort*) deve ser dirigido. Estes incluirão:

(a) Objectivos de Elevado Valor (HVT - *High Value Targets*)

Os HVT são objectivos (forças, meios e capacidades) que o comandante inimigo necessita para a condução bem sucedida de uma modalidade de acção específica. A destruição com sucesso ou a neutralização de HVT degradará seriamente a capacidade do inimigo para continuar com as operações.

(b) Objectivos Remuneradores

Os HPT são objectivos cuja destruição ou neutralização contribui significativamente para o sucesso da operação amiga e para o fracasso da modalidade de acção do inimigo.

Finalmente, determina-se o grau de precisão com a qual um objectivo deve ser batido. Este aspecto consubstancia a Atribuição no Ciclo de *Targeting*.

b. Planeamento e Execução

Depois da informação dos TAI, HVT e HPT ter sido integrada numa JTL pela Célula de *Targeting*, a Célula de Informações vai identificar as necessidades de informação de *targeting* e integrá-las no Plano de Pesquisa. Ao mesmo tempo, a Célula de *Targeting* irá estabelecer os critérios BDA a partir dos quais o grau de eficácia do ataque será deduzido. A Célula das Informações desenvolverá requisitos adicionais de informação a partir desses critérios e irá adicioná-los ao Plano de Pesquisa.

O Gestor da Pesquisa de Informação assegurará que a atribuição de ordens aos sistemas de pesquisa satisfazem as necessidades de informação BDA em coordenação com a fase de execução do Ciclo de *Targeting*.

c. Avaliação

O passo final do Ciclo de *Targeting* consiste na produção de avaliações, pela Célula de Informações, de acordo com os critérios definidos no passo de Planeamento e Execução do Ciclo. Este procedimento irá determinar se o efeito desejado no objectivo foi atingido. Se não tiver sido atingido, toda a informação de *targeting* terá de ser revista para determinar que outras acções devem ser tomadas antes de rever o Ciclo de *Targeting*.

0453. Conclusão

Os processos de informações e de *targeting* estão intimamente relacionados. O *targeting* usa os passos de Direcção e Pesquisa e, em menor escala, o de Processamento do Ciclo da Produção da Informação para obter informações de *targeting* e para conduzir a BDA. As células de informações e de *targeting* irão, por vezes, fazer uso de recursos comuns. Nestas alturas haverá necessidade de decisões do comando, de forma a determinar a distribuição dos recursos existentes. A organização do QG tem que prever estas situações e fazer-lhes face.

O processo de *targeting* permitirá um uso mais eficaz do poder de fogo, ou de outras acções, em apoio ao cumprimento da missão. Para tal, tem de existir, desde logo, uma arquitectura eficiente de informações em apoio a um sistema ISTAR devidamente estruturado. Em operações multinacionais, o uso de uma doutrina e procedimentos comuns, tanto para o processo de informações como o de *targeting*, é essencial para a condução do Processo de *Targeting*.

SECÇÃO VII – O ESTUDO DA SITUAÇÃO DE INFORMAÇÕES

0454. Objectivo

O Estudo da Situação de Informações consiste numa avaliação, escrita ou oral, das informações disponíveis sobre uma dada situação ou condição específica, com vista à determinação das possíveis modalidades de acção de um inimigo, potencial ou não, e a ordem provável da sua adopção. O seu objectivo principal é fornecer ao comandante

PDE 2-00 Informações, Contra-Informação e Segurança

uma base fiável que o apoie na tomada da decisão acerca das operações. O objecto do Estudo da Situação de Informações, como já referido, é analisar a situação do inimigo e avaliar as suas capacidades, prováveis intenções e prováveis modalidades de acção¹⁴, num determinado momento.

0455. Metodologia

A criação de um Estudo da Situação de Informações é um processo que compreende uma análise da situação e uma avaliação. Requer processos de pensamento analítico e lógico. Os métodos e a sequência das suas fases podem variar de acordo com a influência da tradição militar, treino e formação das diferentes nações. O resultado, no entanto, tem de estar conforme as necessidades de informações para o comandante, que são:

- a. Uma avaliação das capacidades do inimigo e prováveis intenções, com base nas informações disponíveis;
- b. A identificação das prováveis modalidades de acção do inimigo, bem como a ordem de probabilidades da sua adopção, caracterizadas segundo um grau de probabilidade de ocorrência e um grau de perigosidade para as nossas forças.

0456. Factores a considerar

Quando se está a desenvolver um Estudo da Situação de Informações, deve atender-se aos seguintes factores:

- a. A missão.
- b. As Características da Área de Operações (clima, condições meteorológicas, efemérides, terreno e outros).
- c. A situação geral do inimigo, a sua conduta até ao momento, as actividades e as capacidades de incluir possíveis reforços, e quaisquer forças na área adjacente, que sejam capazes de influenciar as operações na Área de Interesse do comandante (dispositivo, composição, potencial de combate, actividade recente e actual, aspectos característicos e pontos fracos).

¹⁴ Isto inclui todas as potenciais ameaças, desde actividades criminais a terrorismo.

- d. As possibilidades do inimigo, que incluem as opções e possíveis modalidades de acção (m/a), incluindo nas áreas adjacentes; bem como as suas prováveis intenções, incluindo os seus fins e objectivos em operações imediatas e seguintes.
- e. As conclusões, que contêm a interpretação final do oficial de informações dos elementos apresentados, analisados e sintetizados nos factores anteriores. Estas conclusões proporcionam parte dos dados necessários à escolha de uma M/A pelo comandante.

0457. Princípios

Para prevenir a especulação como princípio básico, as avaliações têm de ser baseadas nas melhores informações possíveis. Podem-se assumir pressupostos quando existirem lacunas. Para evitar mal-entendidos, os pressupostos devem ser sempre claramente identificados como tal. A consistência lógica de pensamento e uma clara separação dos factos em relação aos pressupostos são essenciais para a produção de uma avaliação fiável.

O Estudo da Situação de Informações resulta numa previsão baseada em graus de probabilidade. É uma série de deduções lógicas retiradas da informação disponível e influenciada pelo conhecimento e a experiência do autor. Tem de haver sempre uma estreita ligação entre as células das informações e das operações, especialmente quando se consideram as PIR e ao preparar as necessidades de informação que daí resultam e que irão determinar o Estudo da Situação.

Muitos factos e conclusões do Estudo da Situação de Informações serão também usados numa apreciação operacional, por exemplo, de pontos fortes, capacidades, vulnerabilidades e intenções do inimigo, possíveis m/a e a mais provável.

0458. Orientação Adicional

- Ao analisar uma dada situação do inimigo e os resultados que conseguiu, deve-se pôr a hipótese de deduzir as suas intenções a partir das suas actividades passadas.
- Ao analisar as actividades actuais e avaliar as capacidades inimigas, o enfoque deverá ser colocado na disponibilidade em termos de intenções, pontos fortes, tempo e espaço, prontidão de combate, efectividade de combate e terreno.

PDE 2-00 Informações, Contra-Informação e Segurança

- Ao analisar as opções em aberto em relação a um inimigo em concreto, as suas prováveis m/a e intenções, é recomendável olhar para a situação a partir do seu ponto de vista, tendo presente aquilo que ele possa saber acerca da nossa própria situação. Isto exige um conhecimento aprofundado da mentalidade do seu comandante, da sua organização, padrões de actividade, táctica e hábitos. Todos os factores que afectem as suas capacidades e operações devem ser considerados para incluir uma comparação de forças de um ponto de vista inimigo. Deve-se supor que o comandante tem um conhecimento razoável das nossas capacidades, intenções e vulnerabilidades, se bem que isso possa ser alterado através de manobras de decepção.
- Ao analisar as possíveis futuras intenções adversárias, deve-se ter em consideração a sua situação geral e quais as intenções que foram identificadas até ao momento. Uma vez que o Estudo da Situação de Informações é baseado em supostos objectivos, poderá ter que ser feita uma série de estudos em separado, cada uma delas baseada em objectivos divergentes.
- Ao avaliar as prováveis intenções de um inimigo, e provável m/a, deve-se referir sempre a ordem de probabilidades da sua adopção.
- Diferentes nações poderão usar diferentes sequências quando preparam Estudos da Situação de Informações, mas os princípios gerais mantêm-se iguais.

0459. O Estudo da Situação de Informações e o Estudo Conjunto do Espaço de Batalha pelas Informações

Em geral, o processo formal de Estudo de Situação de Informações será conduzido a níveis mais elevados de comando onde não existem constrangimentos temporais e onde estão disponíveis estados-maiores apropriados para levar a cabo o processo de Estudo de Situação. Um Estudo de Situação de Informações poderá, por exemplo, fazer parte de um Plano de Campanha.

O JIPB é mais susceptível de ser conduzido a níveis mais baixos de comando, em que o tempo é essencial e as prioridades operacionais são mais prementes.

SECÇÃO VIII – APOIO DAS INFORMAÇÕES A OPERAÇÕES DE CONTRA-TERRORISMO

0460. Generalidades

- a. A crescente prontidão de organizações com motivações religiosas e criminais para se envolverem em actos de terrorismo extremo internacional, de modo a conseguirem os seus fins, traz uma nova dimensão às operações de CT. Estas têm de ser tanto conjuntas como multinacionais e têm de cobrir todo o espectro do conflito. Requerem que as forças armadas das nações trabalhem em estreita colaboração com outras entidades governamentais, para desenvolver novas tácticas e novas capacidades na sua luta contra o terrorismo.
- b. O princípio fundamental das operações de CT é que necessitam de informações atempadas e precisas para serem bem sucedidas. Ao contrário da luta armada convencional ou das CRO, em que os oponentes ou os beligerantes são claramente visíveis, o terrorista procura o anonimato e opera dentro da estrutura da sociedade. Contrariamente ao conjunto de necessidades de informações normais, nestas operações é conhecido o objectivo principal do terrorista, uma vez que este publicita a sua causa e as suas exigências são conhecidas. As PIR resultarão, então, da necessidade de saber **quem** é o terrorista, **onde** é que ele se esconde e **qual** irá ser o seu próximo objectivo.
- c. Devido aos recursos financeiros relativamente escassos que os grupos terroristas dispõem e porque a estrutura de células adoptada pelos terroristas normalmente envolve apenas um número reduzido de terroristas, a maioria dos actos de terrorismo são dirigidos a alvos terrestres pouco complexos e com grande visibilidade. No entanto, alguns acontecimentos do passado, tais como ataques a navios e o desvio de aviões comerciais, demonstraram a capacidade dos terroristas operarem tanto contra alvos marítimos como aéreos. O apoio das informações às operações de CT tem por isso de ser considerado de forma igual no contexto das operações de CT conduzidas em meios terrestres, aéreos e navais.
- d. Na sua essência, as informações em apoio às operações de CT derivam dos mesmos processos que qualquer outro tipo de operação. Há, no entanto, diferenças

PDE 2-00 Informações, Contra-Inteligência e Segurança

de ênfase dentro do processo de informações no contexto do CT. Esta secção irá destacá-las e explicar como é que elas afectam a condução do processo de informações nas operações de CT.

0461. Restrições Nacionais

As leis que cobrem o uso de forças nacionais para combater o terrorismo, tanto no interior do próprio país como integradas em operações no estrangeiro, variam entre as diferentes nações OTAN. Este aspecto tem de ser tido em consideração durante o OPP, de forma a assegurar que os componentes nacionais dentro da força OTAN estão a operar dentro das respectivas leis nacionais. Este aspecto poderá impor constrangimentos de interoperabilidade e deve ser considerado na fase inicial.

0462. A Natureza da Informação de Contra-Terrorismo

As informações produzidas em apoio às operações de CT são produzidas de acordo com os princípios das informações através da condução do processo de informações que é, por sua vez, baseado no Ciclo da Produção da Informação. Até aqui, não há diferenças na derivação das informações de CT. Existe, no entanto, uma particular ênfase em certos aspectos das informações produzidas e no processo de informações que é conduzido em apoio às operações de CT:

a. Oportunidade

Um elemento chave no potencial dos terroristas é o factor surpresa. De forma a anular essa vantagem, as informações têm de chegar com oportunidade, quase em tempo real, para permitir à força amiga antecipar a actividade terrorista planeada e adquirir o factor surpresa na condução das operações de CT. A acção atempada é obtida pela integração de um estado-maior bem treinado, que utiliza os procedimentos estabelecidos de forma correcta, dentro de uma arquitectura de informações bem concebida e apoiada.

b. Detalhe

Uma vez que os terroristas poderão conduzir as suas operações em pequenos grupos, maximizando a sua segurança ao operar dentro de uma estrutura de células e ao não manter bases fixas, as suas organizações são difíceis de detectar e de localizar. O desenvolvimento de IR muito específicas é de particular importância na identificação dos terroristas e da actividade terrorista. Um conhecimento abrangente da organização terrorista específica, será um pré-

requisito tanto no desenvolvimento dessas IR como na análise da informação resultante. Isto permitirá que o produto das informações seja suficientemente detalhado, para permitir o planeamento e a condução de operações de CT, com alvos bem definidos, com melhores hipóteses de sucesso, do que operações mais abrangentes, baseadas em informações menos específicas.

c. Ajustado

Na sequência do parágrafo anterior, o detalhe das informações tem de ser ajustado tanto ao ambiente operacional como à operação específica. A capacidade de ajustar as informações tem a sua origem, mais uma vez, de uma compreensão profunda do terrorista e do seu *modus operandi*, tanto da parte da secção de CCIRM da célula de informações, como das outras secções e de outros estados-maiores. O ajuste das informações contribuirá, ao eliminar informações supérfluas ou irrelevantes, para a oportunidade das informações.

d. Gestão da Pesquisa

De modo a satisfazer as necessidades de informação das operações de CT da forma mais rápida e precisa, a célula de informações tem de possuir uma compreensão total das capacidades, não apenas dos meios de pesquisa sob comando do JFC, mas também dos recursos nacionais e estratégicos disponíveis dentro da AO. Também devem ser conhecedores de todos os outros meios de pesquisa que possam ser aplicados, dentro de tempo disponível para a pesquisa da informação, e de quaisquer preparativos especiais para as determinar.

e. Apoio da Nação Hospedeira

O local onde a Força Tarefa Conjunta (JTF – *Joint Task Force*) se encontrar, num papel expedicionário, para conduzir operações de CT noutro país, tem de estabelecer uma ligação com as entidades governamentais dessa nação, de modo a que possam providenciar o Apoio da Nação Hospedeira (HNS – *Host Nation Support*). Estas entidades são uma origem válida de informação específica do país e dos terroristas, a partir da qual o QG da JTF pode desenvolver a sua própria base de conhecimento. Serão também capazes de complementar os meios HUMINT, nas quais a gestão da pesquisa depositará especial confiança.

0463. Origens de Contra-Terrorismo

As informações de apoio às operações de CT derivam de um vasto leque de origens, sendo as principais as seguintes:

a. Informação Humana (HUMINT)

Normalmente, considerando a tática terrorista de se esconderem entre a comunidade, a HUMINT irá desempenhar o papel mais importante na pesquisa de informações de apoio às operações de CT. As operações HUMINT requerem conhecimentos específicos, em que um dos mais importantes é o domínio de uma capacidade linguística credível. Tal capacidade, no entanto, não se desenvolve no imediato. Desta forma, a formação de conhecimentos linguísticos apropriados tem de fazer parte de um desenvolvimento a longo prazo da capacidade HUMINT. Este constrangimento de recursos pode ser facilitado, até certo ponto, através do HNS. No entanto, há que ter certos cuidados ao usar elementos de pesquisa da HNS HUMINT, devendo ser acautelada a possibilidade de que os elementos recrutados não façam parte de um plano de decepção terrorista. A informação obtida por essas origens tem, sempre que possível, que ser confirmada por outras origens. As informações obtidas por meios de reconhecimento e vigilância desempenharão um papel importante no planeamento e condução de operações, mas é provável que o principal relevo recaia sobre a componente HUMINT da força de CT.

b. Informação de Imagens (IMINT)

Nas operações de CT, a IMINT limita-se basicamente à identificação e ao *targeting* de bases terroristas, áreas de treino, esconderijos de equipamento e munições, locais de encontro e rotas de passagem. A tecnologia em evolução torna possível a emissão, em tempo real, de IMINT, para localizar indivíduos e grupos terroristas. Daqui resultará o facto da IMINT ganhar maior relevância nas operações de CT, num futuro próximo.

c. Informação de Transmissões Electromagnéticas e Comunicações (SIGINT)

A SIGINT explora as fraquezas das táticas terroristas pelo facto de, apesar de operarem numa discreta estrutura de células, continuarem a precisar de estabelecer contactos para coordenar as suas operações, anunciar os seus sucessos e emitir as suas exigências. Utilizando o espectro electromagnético, as células ficam expostas às actividades de pesquisa dos meios SIGINT. Os actuais

meios SIGINT conseguem produzir dados exactos de *targeting* permitindo accionar meios de apoio de fogos, quase em tempo real.

0464. Bases de Dados de Informações e Software

Devido à relativa falta de visibilidade dos terroristas, existe uma necessidade de armazenar e aceder a quantidades muito elevadas de informação, de modo a poder identificá-los. Isto requer o desenvolvimento e gestão de bases de dados virtuais. Estas consistem numa quantidade de bases de dados ligadas entre si por uma rede, acedidas por motores de busca e operando como uma base de dados única. Em muitas nações existem ligações (*links*) entre bases de dados militares e outras entidades governamentais, de modo a alargar a busca de informação. As bases de dados virtuais são acedidas por aplicações capazes de ajudar o analista a visualizar informação de modo a retirar informações importantes. As aplicações para efectuar Identificações de Padrões e Análise de *Links* adequam-se à identificação de terroristas e de actividade terrorista.

0465. Estudo Conjunto do Espaço de Batalha pelas Informações

O processo de JIPB é de considerável utilidade em operações de CT. No entanto, devido à natureza assimétrica das operações terroristas e à falta de uma doutrina terrorista identificável, a metodologia tem de ser modificada para ir ao encontro das necessidades das operações de CT. Do mesmo modo que, na sua utilização operacional mais convencional, a resposta do JIPB será expresso numa série de transparentes. As principais mudanças em relação ao JIPB “normal” são:

JIPB normal	JIPB de CT
Avaliação do Espaço de Batalha	Não existem diferenças em relação à avaliação JIPB normal, apenas uma maior concentração em assuntos, tais como clivagens étnicas e sócio-económicas. A análise do mapa identificará possíveis bases terroristas e potenciais alvos terroristas. A análise do terreno indicará a natureza de operações de CT amigas. Nesta fase, a organização dos meios ISTAR podem ser consideradas.
Avaliação da Ameaça	Devido à natureza assimétrica do inimigo, só está disponível uma informação doutrínaria muito limitada. No entanto, com base na experiência de táticas terroristas, o normal processo JIPB pode ser seguido em larga medida: Identificação da Ameaça;

PDE 2-00 Informações, Contra-Informação e Segurança

JIPB normal	JIPB de CT
	Identificação do <i>modus operandi</i> , usando técnicas como a Análise de <i>Links</i> e a Análise de Acontecimentos.
Integração da Ameaça Transparentes de Situação	Nesta fase do JIPB, os factos conhecidos sobre o <i>modus operandi</i> dos terroristas e os potenciais alvos podem ser associados à Avaliação da Área do Espaço de Batalha, de modo a identificar possíveis modalidades de acção inimigas.
Integração da Ameaça Transparente de Acontecimentos	Aqui, as modalidades de acção inimigas são associadas a potenciais objectivos e possíveis NAI, tais como objectivos, rotas para e de objectivos, pontos de conflitualidade, possíveis localizações de emboscadas, esconderijos de armamento, casas seguras, veículos e personalidades que podem começar a ser identificados e apresentados no Transparente de Acontecimentos. PIR, IR e o Plano de Pesquisa começam a ser identificados e desenvolvidos. A Avaliação da Ameaça é conduzida e os planos de FP começam a ser implementados.
Integração da Ameaça Transparente de Apoio à Decisão	As NAI foram aperfeiçoadas de modo a produzir TAI e DP mais específicos. Estes podem ser associados a alvos terroristas específicos identificados a partir dos Transparentes de Situação e de Acontecimentos, pelo movimento ou associação de personalidades ou pelo movimento de veículos. Em operações de CT, os DP poderão ser usados para desencadear uma operação de CT específica, pré-planeada, com a actividade subsequente centrada nos TAI relacionados, em vez de uma nova fase de uma operação decorrente, tal como em operações convencionais. As IR derivadas do Transparente de Apoio à Decisão foram desenvolvidas para atribuição de tarefas para meios de pesquisa ISTAR que cobrem os TAI e DP.

Apesar da inexistência de uma doutrina para operações assimétricas, o JIPB tem um papel chave a desempenhar no planeamento e na conduta de operações de CT. Os procedimentos do JIPB normal, quando usados em conjunto com ferramentas de visualização tais como a Análise de *Links*, Análise Nodal e Análise de Acontecimentos, permitem o desenvolvimento de modalidades de acção e a subsequente identificação de TAI e DP e permitem o planeamento e conduta eficaz de operações de CT.

0466. Informações, Vigilância, Aquisição de Objectivos e Reconhecimento

O processo ISTAR é conduzido exactamente da mesma maneira nas operações de CT como nas operações convencionais. A única diferença significativa será que neste tipo

de operação, como já foi apresentado, poderá haver uma forte base de apoio nas HUMINT. Devido à incerteza das operações terroristas, o contributo que o ISTAR proporciona ao ritmo das operações convencionais traduz-se como igual vantagem na condução de operações de CT. Os tempos de resposta da reacção ao “desencadeamento” dos DP encurtarão e, tal como em operações convencionais, permitirão ao comandante operar dentro do ciclo de decisão/acção dos terroristas.

0467. Targeting

O processo de *targeting* é aplicável de igual forma às operações de CT e às operações convencionais. Para além das infra-estruturas terroristas, o *targeting* nas operações de CT também se aplica a indivíduos. Devido à natureza das organizações terroristas, o *targeting* e a identificação de um terrorista pode ter um efeito desproporcional no modelo global do terrorismo numa AO. No entanto, para conseguir isto, o processo de *targeting* tem de ser conduzido de forma rápida e tem de se basear em informações as mais exactas e atempadas possíveis. Quando o objectivo de *targeting* é um indivíduo ou grupo de indivíduos, alguns meios de pesquisa poderão ter que ser dedicados em exclusivo a essas tarefas, dando origem a um plano de pesquisa específico. Neste caso, o JFC terá um papel chave a desempenhar no processo de Avaliação de Riscos e tem de decidir qual a percentagem de meios de pesquisa a empenhar nesta tarefa específica e tem de avaliar qual a informação que poderá deixar de recolher e quais as implicações que isso poderá ter para a FP.

SECÇÃO IX – AS INFORMAÇÕES NAS OPERAÇÕES DE RESPOSTA A CRISES

0468. Introdução

De uma forma geral, nas CRO, as partes envolvidas terão a propensão para suspeitar de todas as actividades de recolha de informações. A forma de pesquisar informação deverá ser avaliada caso a caso dependendo da forma como progride a operação, da postura dos inimigos e da situação política tanto na área de operações como nos países contribuintes com forças para a operação.

0469. Informações, Vigilância, Aquisição de Objectivos e Reconhecimento

O sistema de Informações, Vigilância, Aquisição de Objectivos e Reconhecimento (ISTAR – *Intelligence, Surveillance, Target Acquisition and Reconnaissance*) é empregue em apoio das CRO, mas a selecção dos meios de pesquisa é influenciada

PDE 2-00 Informações, Contra-Informação e Segurança

pelas particularidades da situação que podem ser alteradas diariamente ou mesmo hora a hora. A célula das informações deve por isso ser bastante flexível na gestão do processo das informações.

0470. Informação Humana

A Informação Humana (HUMINT – *Human Intelligence*) é a mais importante fonte de informações na maioria das CRO. No topo das prioridades de planeamento do comandante do TO deve estar a necessidade de projecção de órgãos de pesquisa HUMINT adequados desde o estágio inicial da CRO.

0471. Necessidades de Informações

As Necessidades Prioritárias de Informações (PIR – *Priority Intelligence Requirements*) no âmbito das CRO são mais abrangentes e politicamente mais complexas que as das operações convencionais. A recolha de notícias e informações terá uma série de áreas de interesse, pelo que a célula de informações fará avaliações relacionadas quer com a força, quer com os vários grupos inimigos. A complexidade das necessidades de informações exige que a Célula de Informações e a Secção de Gestão das Necessidades de Informações e Coordenação da Pesquisa (CCIRM – *Collection Coordination and Intelligence Requirements Management*) possuam competências que permitam transformar os PIR em Necessidades de Informação (IR – *Information Requirements*) e efectuar as respectivas ordens e pedidos de pesquisa.

0472. Indicadores

Os indicadores convencionais são, em grande medida, irrelevantes nas CRO e a célula de informações desenvolverá um leque de outros indicadores, muitas das vezes não convencionais, no sentido de avaliar com rapidez as alterações da situação. O comandante de uma CRO necessitará de notícias e informações sobre uma larga variedade de assuntos para além daqueles sobre os quais as informações são normalmente solicitadas, incluindo:

- A situação geopolítica.
- Os antecedentes históricos, étnicos e culturais que levaram à operação e as prováveis influências de cada um destes factores.
- Avaliações das intenções, atitudes e objectivos de longo prazo de todos os grupos e sub-grupos envolvidos na CRO, tanto relativamente à força como aos outros.

- Avaliações das atitudes e influências da política externa, financeiras, religiosas ou territoriais de grupos com interesse na CRO.
- Atitude dos *media*.
- Influências estratégicas.
- Assuntos civis.
- Economia dos países da área de operações.

0473. Planeamento

A condução do processo das informações nas CRO coloca à célula de informações um conjunto de problemas muito diferenciados daqueles que normalmente se colocam num cenário convencional. A dependência da HUMINT e CI, a grande variedade das necessidades de informações e uma situação operacional imprevisível e volátil, com as suas dimensões geopolíticas, social e económica, colocam desafios constantes à condução do processo das informações.

Deve ser claramente entendido que o planeamento avançado, no que respeita às informações nas CRO, possui tanta ou mais importância do que nas operações convencionais. Nas CRO, o inesperado acontece na maior parte das vezes e as informações devem ter a capacidade e flexibilidade de prever quando acontecerá.

Página intencionalmente em branco

CAPÍTULO 5 ARQUITECTURA DO SISTEMA DAS INFORMAÇÕES

SECÇÃO I – A ARQUITECTURA DAS INFORMAÇÕES NA OTAN

0501. Generalidades

A Arquitectura das Informações na Organização do Tratado do Atlântico Norte (OTAN) (NWIA - *NATO-Wide Intelligence Architectures*) engloba as organizações, processos e sistemas interligados de órgãos de pesquisa, bases de dados, aplicações, produtores e utilizadores de informações. A NWIA facilita a gestão das informações, possibilita as Informações, Vigilância, Aquisição de Objectivos e Reconhecimento (ISTAR - *Intelligence, Surveillance, Target Acquisition and Reconnaissance*), incluindo a conduta do processo da Gestão das Necessidades de Informações e Coordenação da Pesquisa (CCIRM - *Collection Coordination and Intelligence Requirements Management*)) e optimiza as funções das informações a todos os níveis da força, componente ou unidade.

0502. Princípios

O estabelecimento e gestão de uma arquitectura de informações baseia-se nos seguintes princípios:

a. Primazia

A condução do esforço das informações é da responsabilidade do comandante operacional.

b. Flexibilidade

A arquitectura das informações deverá ser:

- (1) Estabelecida e praticada em tempo de paz, permitindo uma rápida transição para operações.
- (2) Capaz de uma rápida reconfiguração para responder a alterações das necessidades de informações durante a conduta das operações.
- (3) Configurada de modo a apoiar o planeamento e conduta das operações a todos os níveis de comando.

c. Interoperabilidade

- (1) Os sistemas de informações e as comunicações existentes em toda a arquitectura, devem permitir a partilha da informação e uma interacção directa. Esta interoperabilidade deve incluir não só os sistemas de informações, mas também os sistemas de C2 a apoiar.
- (2) Os produtos das informações devem ser difundidos em formatos e terminologia comuns aos utilizadores.
- (3) Deverão existir procedimentos que permitam a troca de notícias e de informações que possam ser partilhadas, incluindo:
 - (a) Uma norma comum que permita aos sistemas de tecnologia de informação trocar notícias e informações ao longo de toda a arquitectura.
 - (b) Sistemas de segurança criptográfica comuns.
 - (c) Normas comuns para a conduta do processo da produção da informação que assegurem produtos coerentes.
 - (d) O uso de formatos e terminologia comuns para prevenir equívocos e evitar ambiguidades.

d. Segurança

- (1) A segurança consiste na transmissão atempada de notícias ou informações, de forma adequada e através dos meios convenientes, àqueles que dela necessitam. As informações devem ser disseminadas até ao mais baixo nível de classificação de segurança estabelecido. Se for necessário a sua disseminação a entidades sem a classificação de segurança adequada, só a entidade que a disponibilizou é que pode permitir a sua disseminação a essas entidades.
- (2) Parceiros da Aliança ou de Coligações devem ser considerados no processo de disseminação através de acordos bilaterais e/ou revistos por oficiais de divulgação externa.

e. Acessibilidade

- (1) A arquitectura de informações deve possibilitar o acesso às bases de dados quando apropriado.

- (2) A responsabilidade pela manutenção das bases de dados incluídas na arquitectura das informações, incluindo a leitura, escrita e permissão de acesso às mesmas, deve estar claramente definida.

0503. Capacidade de Comunicações

Os canais de comunicações que deverão existir nos sistemas da arquitectura de informações constituem a chave para o sucesso da sua operacionalização. Possibilitam ainda uma operação efectiva do sistema ISTAR. Para o efeito, deverão dispor de:

- a. Largura de banda suficiente para comportar grande volume de dados.
- b. Redundância para proteger a arquitectura contra falhas dos sistemas ou da acção do inimigo.
- c. Capacidade para serem rapidamente reconfigurados, tendo em vista manter a flexibilidade da arquitectura.
- d. Capacidade para trabalhar em conjunto, de forma directa ou por *interfaces*, por forma a garantir comunicações em tempo real.
- e. Segurança apropriada para protegerem a notícia e informações que transportam.

É imperativo que as células de informações definam claramente a arquitectura de informações e coordenem as comunicações com os planeadores dos Sistemas de Informação e Comunicações (SIC) (CIS - *Communications and Information Systems*), de forma a assegurarem que esta comunidade esteja completamente alertada para os requisitos dos sistemas e linhas de comunicações.

0504. Planeamento da Arquitectura

A célula de informações é responsável pelo desenvolvimento do Plano de Gestão das Informações (IMP – *Intelligence Management Plan*) que apoia a missão. Um dos principais aspectos do IMP é o planeamento da arquitectura das informações, o que será estabelecido de acordo com os princípios a seguir enunciados. Ao estabelecer a arquitectura das informações as células de informações assegurarão que:

PDE 2-00 Informações, Contra-Informação e Segurança

- a. Possuem conhecimento da organização da estrutura de informações, incluindo a distribuição dos meios de pesquisa para a operação ou de quaisquer meios estratégicos, tais como as Células Nacionais de Informações (NIC – *National Intelligence Cells*).
- b. A natureza e capacidades dos meios de pesquisa destinados à operação e à organização de Comando e Controlo (C2) são perfeitamente conhecidos.
- c. Todos os potenciais utilizadores dos produtos das informações foram devidamente identificados.
- d. Nenhuma origem de informação, de produção e de disseminação de informações é motivadora de qualquer possibilidade de falha.
- e. A arquitectura pode abranger ao mesmo tempo a orientação e a obtenção de informações e contém mecanismos de controlo que possibilitem que estas funções sejam conduzidas.
- f. A arquitectura deve ser capaz de abranger todos os cenários possíveis ao longo da operação ou da campanha.
- g. A arquitectura deverá garantir:
 - (1) **Capacidade de Sobrevivência.** Os aspectos técnicos da arquitectura devem garantir a sua sobrevivência, assim como da estrutura de comando que apoiam. Se existirem meios vulneráveis a danos ou destruição, então, devem ser previstos outros meios alternativos.
 - (2) **Interoperabilidade.** As células de informações e de operações têm de ser interoperáveis, no sentido de permitir a produção e visualização de uma Imagem Operacional Comum (COP - *Common Operational Picture*) conjunta.
 - (3) **Segurança.** A política para a protecção das notícias e das informações terá de ser desenvolvida no interior da arquitectura. Ao mesmo tempo, a sua estrutura deverá ser divulgada atempadamente, para que seja possível um acesso alargado à mesma, sem comprometer a segurança das notícias e das informações e/ou a quebra de regras para a partilha da informação.

- (4) **Compatibilidade.** Todas as componentes dos sistemas de informações devem ser capazes de receber e partilhar dados, informação e produtos das informações. Esta capacidade deve ser extensível às aplicações, bases de dados e protocolos de comunicações.

O diagrama seguinte demonstra o modelo genérico da arquitectura das informações.

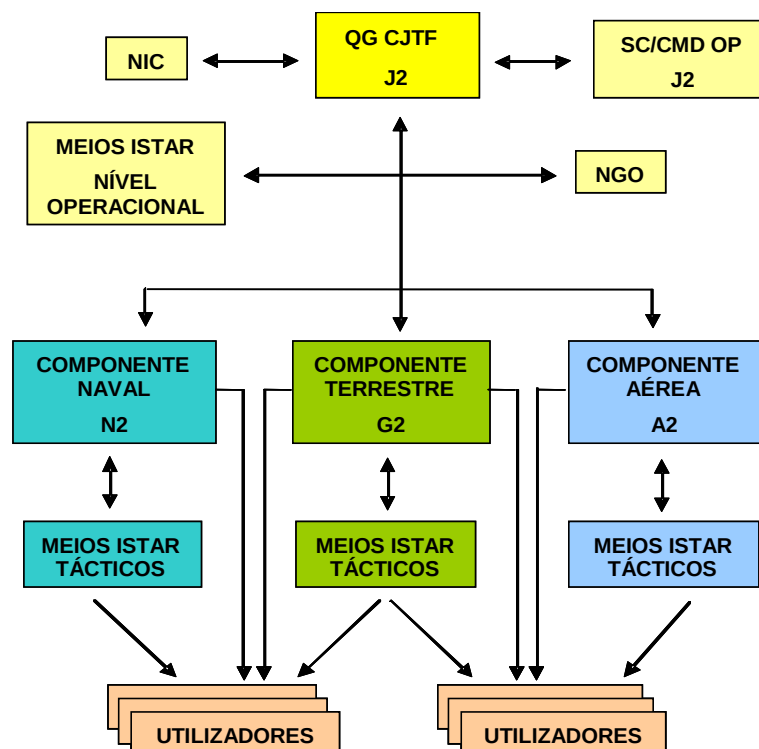


Figura 5-1 – Modelo Genérico da Arquitectura de Informações

SECÇÃO II – CONTRIBUIÇÕES NACIONAIS E MÚLTIPLOS DOMÍNIOS

0505. Generalidades

A NWIA reflecte a contribuição das nações no âmbito das informações através de múltiplos domínios. Um domínio é definido como a combinação de todos os elementos dum sistema, incluindo organização, financiamento, estratégia de gestão, *hardware*, *software*, comunicações, requisitos de segurança e funcionalidades.

0506. Finalidade

A finalidade da NWIA é assegurar a interligação e interoperabilidade entre a OTAN e os sistemas de informações nacionais. Do mesmo modo, a interligação e interoperabilidade entre domínios devem ser alargados a toda a arquitectura de informações.

0507. Funcionalidade

A NWIA disponibiliza total ligação através de correio electrónico (*e-mail*), com ficheiros anexos, e serviços de busca de rede (*web browsing*) entre os domínios em ambiente seguro. Apoia igualmente a transferência de dados e de produtos entre a OTAN e as aplicações nacionais. As aplicações da área das informações fornecidas pela Aliança, são muitas vezes designadas por Serviços Funcionais de Informações (IFS - *Intelligence Functional Services*).

Nas situações onde elementos não-OTAN são envolvidos numa operação, os procedimentos para a partilha da informação com esses elementos devem ser coordenados com a Autoridade de Segurança apropriada.

0508. Grupos Principais de Informações

Os Grupos Principais de Informações são divididos em dois domínios das informações OTAN: o interno e o externo. Apesar destas descrições serem específicas para cada um deles, importa lembrar que todos os domínios estão interligados e garantem interoperabilidade aos serviços de *e-mail* e de *web*.

a. Domínios Internos

A fracção interna da arquitectura de informações da OTAN consiste nas aplicações que a Aliança desenvolve, bases de dados, servidores e estações de trabalho existentes na Rede OTAN Secreta (NATO SECRET WAN - *Wide Area Network*). Existem na NWIA domínios separados destinados a apoiar utilizadores regionais no interior da estrutura de comando da Aliança que operam de forma integrada, tendo em vista o apoio de todos aqueles que produzem informações e dos que a utilizam.

(1) Serviços Centrais

Na OTAN, o termo Serviços Centrais do Sistema Automático de Informação (AIS - *Automated Information System*) refere-se a todas as aplicações de informática que são utilizadas por todas as comunidades de utilizadores, tais como: processadores de texto, manuseamento de mensagens ou apoio geográfico.

(2) Serviços Funcionais de Informações

Na OTAN, o termo Serviços Funcionais de AIS, também designado por IFS, refere-se a todas as aplicações informáticas que são primariamente utilizadas por um serviço, comunidade de utilizadores ou para um propósito específico. Os IFS referem-se às seguintes aplicações:

- (a) *Battlefield Information Collection and Exploitation Systems (BICES) Initial Core Capability (BICC)*. O BICC está a substituir o *Joint Operations Intelligence Information System (JOIIS)* como uma família integrada de bases de dados da OTAN. Estas bases de dados são desenhadas para o armazenamento, recolha, análise, representação gráfica de instalações, unidades, equipamento e pessoas.
- (b) O *Request for Information Management System (RFIMS)* é um sistema para submeter, seguir pistas e procurar informação relativa aos pedidos de informação.
- (c) O *All Source Analysis System (ASAS)* é o sistema do Comando Aliado para as Operações (ACO - *Allied Command for Operations*) destinado a apoiar a pesquisa, preenchimento, produção, armazenamento e recolha por parte dos analistas.

(3) Serviços Funcionais de Não-Informações

É crítico que os IFS da OTAN sejam capazes de partilhar informação com os sistemas de C2 e outros serviços funcionais das componentes apoiadas, para que os dados de informações mais importantes sejam expostos na COP. Correntemente, não existe uma partilha automática e simples da COP e de dados das informações com os sistemas de C2 utilizados pelas componentes aérea e naval. Por sua vez, os meios de informações devem ser partilháveis com o Sistema Conjunto de *Targeting* (JTS - *Joint Targeting System*) o qual é gerido pela componente aérea.

b. Domínios Externos

A parte externa da NWIA consiste nas contribuições de informações nacionais, as quais incluem: redes separadas, servidores, bases de dados e outras aplicações. Estes meios poderão ser fornecidos unilateralmente ou multilateralmente.

(1) O Domínio do BICES

Este domínio consiste em produtos nacionais de informações, apoiados pela ligação e pelos servidores da NATO BICES Agency (NBA). As nações colocam

PDE 2-00 Informações, Contra-Informação e Segurança

a informação em bases de dados nacionais que podem ser acedidas através da rede por utilizadores de toda a NWIA. O BICES disponibiliza e-mail seguro, e utilizando tecnologia web, permite a troca de notícias e de informações até ao nível OTAN SECRETO.

(2) O Domínio EUA

Os EUA contribuem para a OTAN com produtos de informações e serviços separados, ambos de forma directa e via BICES. A combinação da organização de apoio, as redes informáticas, servidores, aplicações e algumas estações de trabalho, são correntemente designadas por *Linked Operational-Intelligence Centres Europe* (LOCE). Este processo encontra-se em fase de mudança, tendo em vista uma ligação alargada com a rede global do *Combined Enterprise Regional Information Exchange System* (CENTRIXS).

0509. Comunicações

Estas WAN separadas encontram-se ligadas entre si, para garantirem a interligação marginal entre os grupos internos e externos. A relação entre os domínios e as comunicações de apoio podem ser observadas na figura seguinte.

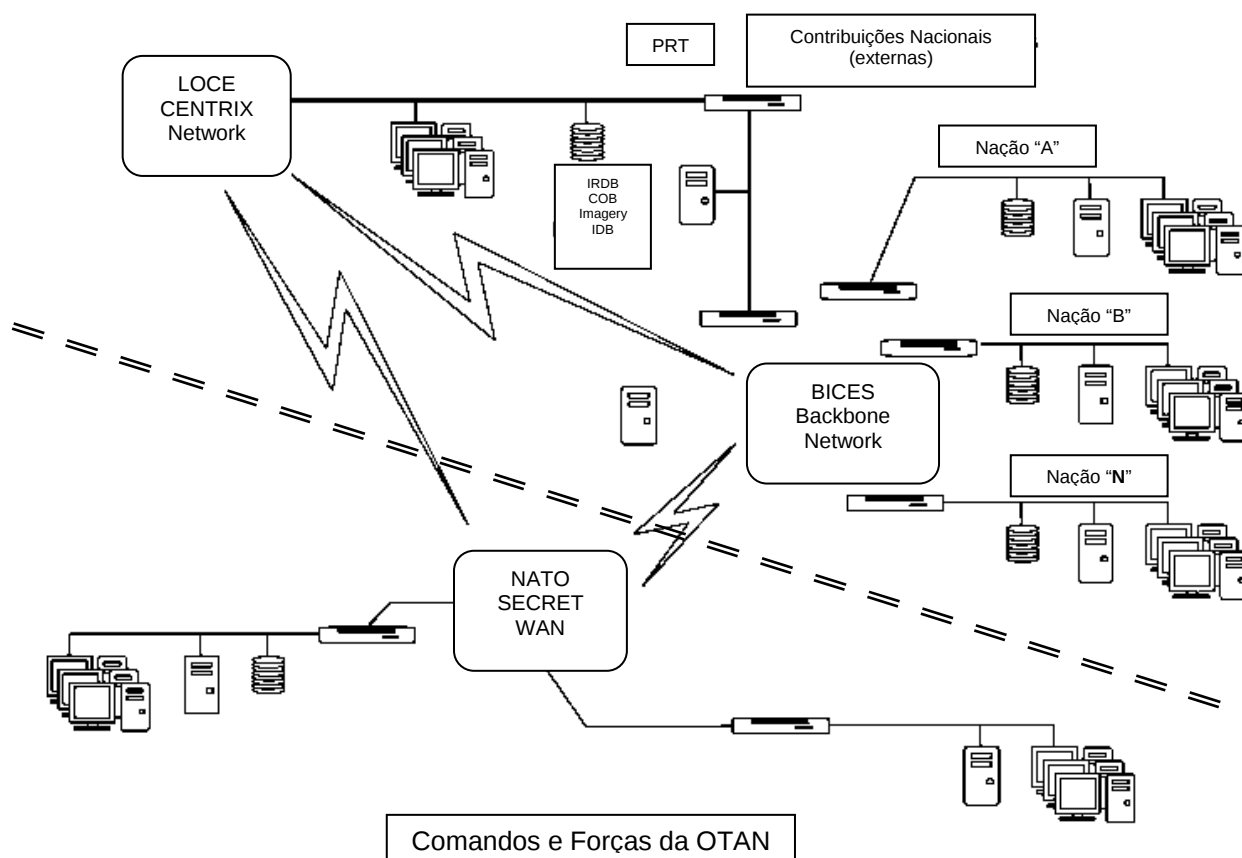


Figura 5-2 – Modelo Integrado da Arquitectura de Informações da OTAN

0510. A Responsabilidade das Células de Informações

No desenvolvimento das arquitecturas de informações para a missão, serão exigidas células de informações de forma a compreenderem os seguintes detalhes relativos à NWIA:

- a. **Missão.** Qual é a principal finalidade de cada sistema (de notícias e de informações) na arquitectura?
- b. **Funções.** Quais as tarefas cometidas aos vários sistemas participantes, aos gestores e como estes se ligam com as informações?
- c. **Projectação.** Quais são as áreas da responsabilidade dos sistemas e qual a melhor forma de serem aplicadas na arquitectura das informações prevista para a operação ou campanha?

SECÇÃO III — O APOIO DOS SISTEMAS DE INFORMAÇÃO GEOGRÁFICA ÀS INFORMAÇÕES

0511. Os Sistemas de Informação Geográfica

Os Sistemas de Informação Geográfica (GIS – *Geographic Information System*) têm por base o *hardware*, *software*, dados, operadores, comunicações e ferramentas analíticas que em conjunto numa organização, pesquisam, armazenam, difundem e exploram dados geodésicos, geomagnéticos, litorais e culturais, rigorosamente referenciados e localizados de forma precisa na superfície terrestre. A informação geoespacial tem um papel significativo nas operações militares, fornecendo a base de toda a restante informação do espaço de batalha. Quando associada com as informações, a informação sobre forças amigas, as condições meteorológicas e a situação logística, os GIS auxiliam o comandante a visualizar o espaço de batalha, durante o planeamento e condução das operações, na navegação e numa aquisição precisa de objectivos inimigos. O sistema utiliza vários tipos de dados georeferenciados, a partir dos quais se adquire camadas de informação a fim de serem reunidos em transparentes sobre mapas electrónicos sob a forma de COP. Os GIS apoiam as informações e outras células de estado-maior durante o Processo de Planeamento Operacional (OPP – *Operational Planning Process*) e são o suporte da metodologia baseada em gráficos, utilizada no Estudo Conjunto do Espaço de Batalha pelas Informações (JIPB – *Joint Intelligence*

PDE 2-00 Informações, Contra-Informação e Segurança

Preparation of the Battlespace). Em qualquer operação conjunta ou combinada, a integração da visão do espaço de batalha de cada componente, constitui um desafio importante para a definição de uma visão única do mesmo. Os GIS constituem a chave para este processo de fusão.

O apoio dos GIS é garantido através dum processo de planeamento, no qual a sua organização:

- a. Identifica a Área de Interesse (AOI - *Area of Interest*).
- b. Determina as necessidades de apoio GIS às informações e outras células de estado-maior.
- c. Define a arquitectura de difusão do GIS.
- d. Determina os recursos GIS disponíveis para satisfazer as necessidades levantadas.
- e. Desenvolve uma estratégia de produção para identificar deficiências e insuficiências dos produtos GIS.
- f. Dissemina os produtos GIS como apropriado.

0512. Os Dados Geoespaciais

Os dados geoespaciais podem ser disseminados de duas formas:

- a. **Hard Copy.** No nível tático das operações, os mapas e cartas constituem o principal método de acesso a dados geoespaciais. Os principais constrangimentos deste tipo de dados relacionam-se com as áreas de produção, transporte e oportunidade da informação.
- b. **Digital.** Dados geoespaciais em formato digital podem estar disponíveis na WAN ou em meios electrónicos sob a forma de CD-ROM que podem ser colocados em servidores de Redes de Área Local (LAN – *Local Area Network*) numa Área de Operações Conjunta (JOA – *Joint Operations Area*).

Os dados geoespaciais de elevada resolução como a imagem rasterizada (*raster imagery*) e mapas, de muito pormenor e densa altimetria são normalmente guardados em grandes ficheiros digitais. A sua transmissão electrónica exige grandes larguras de

banda de comunicações que serão extremamente úteis durante as operações. O comandante deve estabelecer prioridades para o uso destas bandas, mas deve evitar a competição pela sua utilização. Quando possível, devem ser trocados dados geoespaciais digitais através do *Digital Audio Tape* ou CD-ROM.

Os dados geoespaciais digitais apoiam o processo das informações. Apresentam vantagens relativamente aos mapas e cartas analógicas, visto que podem ser integrados nos sistemas de C2 e ajustados de acordo com uma necessidade específica definida por uma célula de informações. Constituem a chave para o sucesso de um alerta situacional através da COP e são a pedra angular durante o OPP.

SECÇÃO IV – BASES DE DADOS DAS INFORMAÇÕES

0513. Formatos

As informações são armazenadas sob dois formatos:

a. Estruturadas

Os dados de informações estruturados são armazenadas em bases de dados nas quais cada registo tem uma estrutura definida que consiste numa série de campos. As informações são extraídas da base de dados através do uso de páginas de *internet*, desenhadas especificamente para aceder a uma estrutura de dados específica.

b. Não-estruturadas

Os dados não-estruturados são armazenados num repositório de dados e, no caso de dados de informações, usualmente na forma de texto. As informações são extraídas do repositório através da utilização de um motor de busca semelhante ao usado num *web browser* para pesquisa de informações indexadas.

0514. Bases de Dados Relacionais

As bases de dados de informações são quase exclusivamente bases de dados relacionais, nas quais, a informação é armazenada sob a forma de relações entre entidades. As relações podem representar, por exemplo: um número de certo tipo de aeronaves num aeródromo, a relação entre um equipamento e o local ou a presença de um determinado oficial com a designação dum regimento ou uma relação entre uma pessoa e uma unidade.

0515. Bases de Dados Normalizadas

Para proceder à troca de dados entre duas bases de dados estruturadas é necessário existir um formato comum. Isto significa que a sua estrutura para enviar e receber deverá ser a mesma. Para o efeito, deverão conter o mesmo título, campos idênticos com formatos iguais e o mesmo tipo de caracteres.

Quando estas condições forem satisfeitas e as ligações de comunicações entre ambas as estruturas de bases de dados forem uma realidade, os dados podem ser enviados ou trocados de uma base de dados para a outra.

0516. A Gestão de Bases de Dados

As células de informações são responsáveis por:

- a. Estabelecer uma arquitectura que permita o acesso a todas as bases de dados que contêm notícias e informações relevantes para a operação ou campanha.
- b. Prever permissões de escrita e leitura para bases de dados destinadas ao pessoal das informações.
- c. Estabelecer uma política para a manutenção das bases de dados através da revisão do armazenamento de notícias e informações na base de dados.
- d. Atribuir classificações de segurança aos dados a serem armazenados numa base de dados.
- e. Permitir a realização de *downloads* de uma base de dados para outras, conforme apropriado.

CAPÍTULO 6 NÍVEL OPERACIONAL DAS OPERAÇÕES

SECÇÃO I – INTRODUÇÃO

0601. Generalidades

- a. O presente capítulo apresenta os conceitos relativos às informações, descreve o enquadramento operacional e a natureza das informações no nível operacional. Examina o apoio das informações ao planeamento e às operações e apresenta as noções inerentes à arquitectura conjunta das informações.
- b. No nível operacional, as forças armadas são projectadas e empregues para alcançar objectivos estratégico-militares e/ou operacionais numa dada área de operações conjunta. Para alcançar os objectivos, as operações têm de ser planeadas no contexto do ambiente do teatro.
- c. A missão das informações consiste em fornecer ao comandante informações que sejam precisas, relevantes, atempadas e utilizáveis. No nível operacional conjunto, as informações centram-se nas capacidades e intenções dos actuais e potenciais inimigos e nos prováveis efeitos que o ambiente pode representar na conduta das operações, quer do inimigo quer das forças amigas. Nesse sentido, as células de informações monitorizam os acontecimentos na área de interesse e apoiam a condução das campanhas.

0602. Operações Conjuntas

As operações conjuntas são definidas como operações nas quais podem estar envolvidos elementos de mais do que um ramo, podendo envolver meios e/ou forças aéreas, espaciais, navais, anfíbias, terrestres ou de operações especiais. Um plano de operações conjunto sincroniza o emprego destas forças sobre os Centros de Gravidade (CoG – *Centre of Gravity*) estratégicos e operacionais dos inimigos. A operação pode integrar forças provenientes de nações OTAN projectadas numa Força Conjunta da Aliança (AJF – *Allied Joint Force*) ou numa CJTF. Neste caso, pode ainda integrar forças de nações contribuintes não pertencentes à OTAN.

Um comandante conjunto está preocupado com o emprego da força como um todo, em todas as fases da operação, desde o conceito ao planeamento e execução, em

PDE 2-00 Informações, Contra-Informação e Segurança

campanhas ou em Operações Conjuntas de Grande Envergadura (MJO - *Major Joint Operations*). Esta força deve contribuir directamente para atingir os objectivos estratégico-militares definidos para a operação. Os comandantes operacionais garantem a ligação entre a orientação proveniente do nível estratégico e a execução ao nível tático.

Os conceitos operacionais chave incluem:

- Sinergia e potenciação;
- Manobra;
- Simultaneidade e profundidade;
- Balanceamento e antecipação;
- Ritmo;
- Gestão do tempo;
- Objectivo;
- Ofensiva;
- Massa;
- Economia de forças;
- Unidade de comando;
- Segurança;
- Surpresa;
- Simplicidade.

0603. Informações Conjuntas

Dispor de informações precisas e atempadas é um factor essencial para a conduta das operações conjuntas, pois representa uma parte determinante das Necessidades de Informações Críticas do Comandante (CCIR – *Commander's Critical Information Requirements*).

SECÇÃO II – NATUREZA DAS INFORMAÇÕES NO NÍVEL OPERACIONAL

0604. Papel das Informações

- a. As informações no nível operacional são necessárias para o planeamento, execução e avaliação das operações no Teatro de Operações (TO) ao nível do QG Conjunto (JHQ – *Joint Headquarters*) e são produzidas na área geográfica do TO.
- b. As células de informações no nível operacional garantem as notícias e as informações sobre o que o inimigo ou potenciais inimigos estão a fazer, o que são capazes de fazer e o que futuramente poderão fazer. As informações auxiliam o Comandante da Força Conjunta (JFC – *Joint Force Commander*) e o seu Estado-Maior (EM) na visualização do espaço de batalha.
- c. As informações no nível operacional apoiam todas as fases das operações militares, desde a projecção das forças até ao emprego, sustentação e retracção. Para além disso, produzem as informações necessárias para o cumprimento dos objectivos estratégicos nos TO e/ou Áreas de Operações Conjuntas (JOA – *Joint Operations Area*), incluindo o apoio ao planeamento e execução das campanhas subordinadas e das MJO.
- d. As informações no nível operacional apoiam todos os aspectos da campanha conjunta. As suas tarefas focalizam-se em prover o comandante com a informação necessária para identificar os CoG do inimigo e garantir informação relevante, atempada e oportuna que possibilite a execução do plano de campanha. Garantem igualmente, o apoio às Operações de Informação (INFO OPS – *Information Operations*).

0605. Finalidade das Informações no Nível Operacional**a. Apoio ao Comandante**

As células de informações apoiam o comandante na determinação de objectivos e no planeamento, execução e avaliação das operações. Apoiam igualmente os comandos subordinados e de forma contínua a Protecção da Força (FP – *Force Protection*). Esta função é coincidente, embora separada, das responsabilidades das células de informações no apoio a outras células, tal como as suas

PDE 2-00 Informações, Contra-Informação e Segurança

responsabilidades na satisfação dos pedidos de pesquisa (RFI – *Request for Information*) das componentes subordinadas.

b. Apoio à Missão

As informações no nível operacional constituem um elemento crucial no apoio à missão. É vital existir Informação especializada sobre as características do equipamento específico e parâmetros de emissão¹⁵ do inimigo, para um apoio em tempo oportuno à missão. Esta exige dados específicos sob a seguinte forma: transparentes de situação - para apoiar os sistemas de planeamento, alerta e de defesa; informação obtida pela guerra electrónica, através de medidas de apoio electrónico, e ainda, dados paramétricos para apoiar os sistemas de reconhecimento automático de alvos.

c. Identificar e Determinar Objectivos

Todos os aspectos das operações militares dependem duma clara definição dos objectivos. No processo de identificação de objectivos, as células de informações devem compreender as responsabilidades do comandante, a sua missão e intenção, meios disponíveis (incluindo forças multinacionais), forças adversárias e as características do ambiente operacional. As informações no nível operacional devem facultar ao comandante um conhecimento do inimigo, em termos da sua provável intenção, objectivos, capacidades, fraquezas, pontos fortes e vulnerabilidades críticas. As células de informações recomendam então atacar as capacidades do inimigo e explorar as suas vulnerabilidades críticas. Logo que o comandante determine os objectivos, as células de informações revêm-nos continuamente tendo em atenção o inimigo e as mudanças de situação para verificar o que permanece relevante para a intenção do comandante. O nível operacional das informações fornece igualmente contribuições para a avaliação das ameaças que constituem a base da FP.

d. Planear e Conduzir Operações

As informações no nível operacional devem ser garantidas em todos os níveis de comando para o planeamento, direcção e condução das operações. Este aspecto é crítico para os comandantes e respectivos EM na identificação e selecção de objectivos específicos e de alvos, bem como na determinação dos meios,

¹⁵ Entende-se como parâmetros de emissão a frequência e o tipo de modulação das emissões.

operações e táticas a serem usadas para alcançar a missão do comandante operacional. As células de informações apoiam então a execução do plano com as informações necessárias para sustentar as operações, adquirir objectivos e proteger as forças amigas. Para manter a iniciativa, o comandante procurará conduzir o ciclo de decisão/acção das operações de forma mais rápida que o seu inimigo, e assim, reagir rapidamente face ao evoluir da situação. As células de informações são uma parte determinante neste processo, respondendo o mais rapidamente possível às Necessidades Prioritárias de Informações (PIR – *Priority Intelligence Requirements*).

0606. Perspectiva Geral das Necessidades de Informações

O conhecimento da situação no espaço de batalha constitui a necessidade que cobre três componentes que se complementam entre si: o inimigo, o ambiente operacional e as forças amigas. As células de informações são responsáveis por fornecer notícias e informações sobre as duas primeiras componentes. Por sua vez, às células de operações compete-lhes prover a terceira. A componente inimigo exige um conhecimento actualizado dos dispositivos e actividades das forças adversárias que operam no espaço de batalha, baseada numa análise detalhada dos efeitos das condições meteorológicas e do terreno. A componente ambiente operacional exige o conhecimento da geografia, clima, factores demográficos e o seu impacto nas operações.

0607. Inimigo

a. Tipo

É essencial o conhecimento do inimigo no que diz respeito à sua liderança política, ideologia, orientações, estruturas, coesão nacional, aspectos psicológicos, moral, tradição, personalidades, história, situação das forças armadas e biografia dos comandantes. Estas informações apoiam a avaliação das intenções e comprometimentos do inimigo, apoio popular, a aquiescência para aceitar baixas e a sua susceptibilidade às Operações Psicológicas (PSYOPS – *Psychological Operations*) e decepção.

b. Capacidades

É igualmente necessário dispor de informações respeitantes à organização e recursos das autoridades civis, a estrutura de comando, ordem de batalha (ORBAT – *Order of Battle*), padrões de treino, doutrina, armamento e equipamento (incluindo

PDE 2-00 Informações, Contra-Informação e Segurança

características técnicas), capacidades das Informações, Vigilância, Aquisição de Objectivos e Reconhecimento (ISTAR - *Intelligence, Surveillance, Target Acquisition and Reconnaissance*) e logísticas das forças armadas. Estas informações apoiam uma avaliação do inimigo em relação às nossas forças, sendo utilizadas, em particular, para avaliar os potenciais relativos de combate, a natureza da ameaça e os pontos fortes e fraquezas do inimigo e suas vulnerabilidades críticas.

c. Localização

Informações sobre a localização do inimigo são indispensáveis para identificar a sua postura e assim, avaliar as suas intenções e grau de ameaça, garantindo um aviso prévio e possibilitando um adequado processo de targeting. Nas Operações de Resposta a Crises (CRO – *Crisis Response Operations*) a distribuição e postura dos agregados populacionais pode tornar-se igualmente importantes.

d. Intenções

Compreender as intenções do inimigo bem como as suas reacções às actividades desenvolvidas pelas nossas forças é fundamental para o sucesso das operações. Este facto confere aos comandantes uma vantagem na preparação e protecção das suas forças e permite-lhes antever as operações do inimigo. Capacita-os igualmente para seleccionar os pontos decisivos (DP – *Decision Points*) nos quais irão concentrar as suas capacidades e esforços nas vulnerabilidades do inimigo, tendo em vista dominar o seu CoG. Relatórios e avaliações são críticas para este requisito.

0608. Ambiente Operacional**a. Geografia/Infra-Estruturas/Aspectos Sanitários**

A geografia terrestre, aérea e marítima, a situação económica, as infra-estruturas e os aspectos sanitários são factores sobre os quais devem ser obtidas informações, tendo em vista uma criteriosa selecção de equipamento, para além de uma preparação, projecção, planeamento, condução das operações e *targeting* eficientes.

b. Clima

As informações referentes à previsão das condições meteorológicas e a sua provável influência nos sensores e plataformas das informações, capacidades de combate, movimento e manobra, pessoal, logística e comunicações, são

necessárias para o treino e preparação da força, para decidir qual o momento mais indicado para a projecção e operações e ainda, para auxiliar a decepção e a surpresa.

c. Demografia

Informações sobre a cultura, língua, religião, leis internas e tradições da população na área de operações são necessárias para auxiliar a preparação da força, o planeamento e conduta das operações. Os avanços tecnológicos no processamento através de computadores, a precisão global geográfica e as telecomunicações melhoram a capacidade do comandante de nível operacional para determinar as localizações das forças amigas e do inimigo, bem como, pesquisar, processar e difundir dados relevantes para numerosos locais. Estas capacidades, combinadas com a aptidão para negar ou degradar a capacidade do inimigo para pesquisar, processar e difundir um ininterrupto fluxo de informação, proporcionará ao comandante superioridade de informação. Do mesmo modo, a fusão de todas as fontes de informação, através da integração de sensores, plataformas, organizações de comando e de centros de apoio logístico, permitirá que a realização de um grande número de tarefas operacionais decorra de forma rápida e providencia um conhecimento mais detalhado do espaço de batalha (uma peça chave da superioridade de informação).

d. Espaço

Operações no espaço, e a partir deste, são cada vez mais importantes. Devido à especificidade das operações neste contexto, estas serão primariamente estratégicas na sua natureza. No entanto, os sensores localizados no espaço terão um impacto nos níveis operacional e tático das operações, por isso, durante o planeamento, o recurso a este tipo de sensores deve ser tido em conta pelas informações e, em simultâneo, deve ser conduzido por forma a contrariar operações desenvolvidas pelo inimigo a partir do espaço.

SECÇÃO III – O APOIO DAS INFORMAÇÕES AO PLANEAMENTO

0609. Generalidades

- a. O planeamento de uma operação é uma função essencial para o JFC. A este compete-lhe dirigir o mesmo e decidir qual a modalidade de acção que será a base do seu plano de campanha. Na OTAN existem duas categorias de planeamento – o **Planeamento Avançado** que consiste em desencadear e desenvolver planos baseados em cenários, antecipando eventos e circunstâncias futuras, às quais a Aliança poderá ter que vir a fazer face (o produto final será a obtenção de um Plano de Contingência ou de um Plano de Defesa Permanente) e o **Planeamento de Resposta a Crises** que consiste em desencadear e desenvolver planos de resposta a crises existentes ou em fase de desenvolvimento (o produto final é um Plano de Operações). Ambos lidam com o desenvolvimento de um plano de campanha que não é mais do que a expressão prática da arte operacional e inclui, entre outros, o estado final, CoG, DP, determinação do esforço, pontos de culminação e estratégias de saída.
- b. O Ciclo da Produção da Informação é um modelo conceptual simplificado de como as operações das informações são conduzidas.
- c. No nível operacional, o Ciclo da Produção da Informação constitui a base de entendimento para uma terminologia, táticas, técnicas e procedimentos comuns. O seu conhecimento é fundamental para entender as actividades das informações descritas no final deste capítulo.
- d. A missão dos comandantes constitui o ponto fulcral para todas as fases do ciclo. As actividades realizadas em cada uma delas são conduzidas continuamente e em conjunto com as que irão decorrer noutras fases.

0610. Processo de Planeamento Operacional

O Processo de Planeamento Operacional (OPP – Operational Planning Process) permite a um JFC preparar atempada e eficientemente os Planos de Operações (OPLAN – *Operational Plans*) de resposta a uma crise actual ou em desenvolvimento. O

OPP é aplicável em qualquer QG do nível Estratégico, Operacional ou Tático. Em geral, o processo consiste em cinco fases.

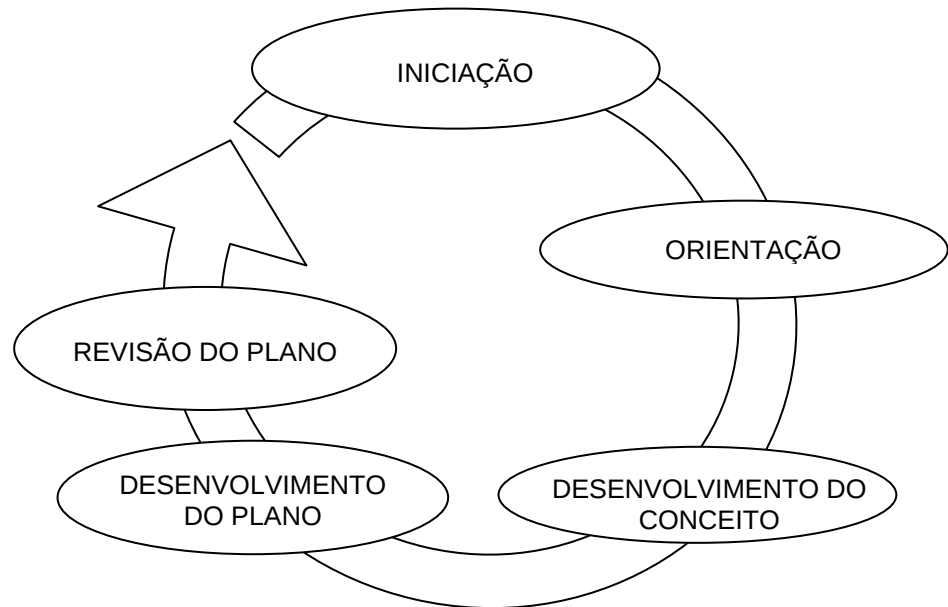


Figura 6-1 – Fases do Processo de Planejamento Operacional

Fases do OPP	Passos	Tarefas das Informações
Iniciação	- Receber a Directiva Iniciadora/Directiva Inicial de Planeamento; - JFC inicia o seu OPP em antecipação à recepção da missão; - JFC organiza o planeamento de EM ou o seu EM fá-lo por ele.	- Receber a Directiva Iniciadora; - Revisão das bases de dados; - Enviar os RFI iniciais; - Rever as capacidades de informação geográfica e antecipar novos requisitos; - Difundir produtos geográficos ao EM; - Integrar o Grupo Conjunto de Planeamento das Operações (JOPG – <i>Joint Operations Planning Group</i>); - Preparar o briefingue inicial para o JOPG (iniciar o JIPB) - Monitorizar a situação.
Orientação	- Directiva Inicial de Planeamento do JFC; - Análise da Missão/<i>Brainstorming</i>; - Restabelecer a missão; - Briefingue da Análise da Missão; - Preparar a Directiva de Planeamento do Comandante (CPG – <i>Commander's Planning Guidance</i>).	- Receber o briefingue inicial do JOPG/JIPB e inseri-lo no Briefingue da Análise da Missão. Focalizar a atenção na situação, intenção do inimigo, projecção, capacidades e limitações, CoG, forças, potenciais modalidades de acção, outros aspectos chave, estado final desejado, principais alvos para as INFO OPS; - Organizar e participar no Briefingue da Análise da Missão; - Assegurar que todo o EM compreende a missão; - Preparar informações ao nível do JFC; - Monitorizar a situação.
Desenvolvimento do Conceito	- Rever a CPG; - Analisar os factores que afectam o desenvolvimento das modalidades de acção, - Desenvolver as modalidades de acção; - Briefingue da Decisão; - Decisão do Comandante.	- Rever a CPG; - Estimativa do EM – incidindo em factores chave do inimigo e identificando outros (políticos, sociais, tempo, espaço, etc); - Desenvolver as modalidades de acção do inimigo e ordená-las de acordo com o grau de probabilidade – no mínimo a mais provável e a mais perigosa (desenvolver outras se o tempo o permitir). As modalidades de acção do inimigo devem ser levantadas tendo em vista atacar o nosso CoG; - Elaborar a matriz de sincronização para cada modalidade de acção do inimigo, - Determinar a técnica a utilizar durante o “jogo da guerra”; - Organizar e conduzir o “jogo da guerra”. Assegurar que os resultados chave do inimigo são devidamente registados; - Registrar todos os DP das nossas forças e antecipar os pedidos de pesquisa para apoiar estas decisões; - Preparar a parte relativa ao Briefingue da Decisão; - Finalizar e difundir as modalidades de acção do inimigo baseadas na Decisão do Comandante; - Desenvolver a Lista de Objectivos de Elevado Valor (HVTL – <i>High Value Targets List</i>) para a ameaça; - Desenvolver as informações relativas ao Targeting; - Auxiliar no desenvolvimento do Conceito de Operação (CONOPS – <i>Concept of Operations</i>). - Elaborar o Anexo das Informações; - Monitorizar a situação.
Desenvolvimento do Plano	- Desenvolver o CONOPS; - Desenvolver o Plano a partir do CONOPS aprovado; - Projecção da Força	- Desenvolver o plano de informações; - Assegurar que o plano de informações está sincronizado com os restantes planos; - Apoiar o Processo de Targeting Conjunto; - Apoiar o desenvolvimento da Lista de Objectivos Remuneradores (HPTL – <i>High-Payoff Targets List</i>); - Aprovar o plano(s) de informações; - Monitorizar a situação durante a projecção.
Revisão do Plano	- Rever o Plano; - Validação do Plano; - Briefingue da Decisão de Revisão ao JFC (se requerido).	- Monitorizar a situação; - Rever o Plano de Pesquisa; - Planos de informações, jogos de guerra, ensaios ou modelos operacionais de pesquisa adicionais; - Apoiar o Briefingue da Decisão de Revisão ao JFC.

Tabela 6-2 – Tarefas das Informações durante o OPP

0611. Estudo Conjunto do Espaço de Batalha pelas Informações

A finalidade principal do Estudo Conjunto do Espaço de Batalha pelas Informações (JIPB – *Joint Intelligence Preparation of the Battlespace*) é apoiar o planeamento de campanha e a tomada de decisão do JFC e dos Comandantes de Componente e assegurar a base para a orientação e sincronização das informações. O JIPB é conduzido prioritariamente para/e durante as operações das forças conjuntas, bem como, durante o planeamento de missões subsequentes.

SECÇÃO IV – APOIO DAS INFORMAÇÕES ÀS OPERAÇÕES**0612. Generalidades**

A possibilidade de um comandante possuir uma visualização precisa do espaço de batalha exige uma coordenação estreita e sincronizada das actividades das informações. Todas estas actividades são conduzidas pelas células de informações e organizações com o propósito de garantir ao comandante informações relevantes, precisas e em tempo oportuno. A eficácia das actividades de informações possibilitam aos comandantes, em todos os escalões, aplicar as forças à sua disposição de forma acertada, eficiente e eficaz, caracterizando-se por um planeamento centralizado e execução descentralizada, procurando maximizar o apoio oferecido ao comandante de nível operacional, enquanto que, simultaneamente, fornecem informações específicas e detalhadas a outros comandantes e respectivos EM de toda a força conjunta.

Particularmente importante, é o facto das informações apoiarem as forças operacionais ao longo da condução das operações militares, inclusive, desde a sua projecção. Para um efectivo planeamento e execução das missões das unidades, o pessoal das informações projectado deverá estar devidamente inteirado do conceito da operação, da arquitectura das informações, do estudo da situação, das cartas da região e de outros factores relativos ao teatro de operações. Os responsáveis pela produção das informações devem difundir-las o mais rapidamente possível às forças a projectar, segundo um formato electrónico normalizado.

0613. Informações, Vigilância, Aquisição de Objectivos e Reconhecimento

O ISTAR no nível operacional coordena o processo das informações e o esforço de pesquisa dos diversos órgãos de pesquisa da força conjunta. Incorpora igualmente o Sistemas de Informação e Comunicação (SIC) (CIS - *Communication and Information*

PDE 2-00 Informações, Contra-Inteligência e Segurança

Systems) que o apoia. O sistema ISTAR focaliza-se na Área de Responsabilidade de Informações (AIR - *Area of Intelligence Responsibility*) do JFC e é igualmente responsável por identificar a sua AI.

O sistema ISTAR conjunto deve permitir detectar, localizar e identificar as forças de combate adversárias. A identificação e localização dos CoG inimigos, nós críticos, principais eixos, segundos escalões e armas de destruição maciça serão prioritários. Para outro fim do espectro do conflito, o sistema ISTAR deve permitir identificar e localizar personalidades chave e determinados indivíduos, centros críticos de actividade e células operativas e/ou grupos. A protecção das nossas forças, do reconhecimento e vigilância por parte dos meios de pesquisa do inimigo, constitui igualmente uma elevada prioridade.

O ciclo da produção da informação apoia o ISTAR. A orientação é a chave para uma eficiente utilização das células de informações e dos órgãos de pesquisa, e a pesquisa de dados é crítica para o desenvolvimento de medidas e sistemas de alerta. O processamento é executado em todos os órgãos de análise e as notícias e as informações são disseminadas para aqueles que delas necessitam. Consequentemente, o *targeting* conjunto é apoiado pelos processos das informações e do ISTAR.

0614. O Processo de *Targeting* Conjunto**a. Aplicação do Processo**

Este processo inicia-se e prolonga-se ao longo do OPP. Pode ser utilizado em tempo de paz e em situação de conflito. As informações apoiam o *targeting* através da identificação das capacidades do inimigo e dos sistemas que podem ser designados como objectivos e, ainda, pela análise dos efeitos das armas e da avaliação de danos no espaço de batalha.

b. Os objectivos são considerados de acordo com os seguintes grupos:**(1) Estratégicos**

São objectivos que, se forem atacados podem afectar a capacidade do inimigo a longo prazo, bem como a sua vontade de manter as hostilidades (exemplos: capacidade C2 estratégica, infra-estruturas económicas, fundos de organizações terroristas ou alvos que possam ter implicações para a população). Por definição, todos os objectivos associados a armas de destruição maciça ou de energia nuclear são considerados estratégicos.

(2) Operacionais

São objectivos que, se forem atacados afectam a capacidade militar do inimigo (sistemas de defesa aérea, depósitos de munições ou depósitos de armamento de organizações terroristas) ou condicionam directamente a sua capacidade de sustentação das hostilidades (linhas de comunicações ou bases seguras).

(3) Tácticos

São objectivos que, se forem atacados afectam a capacidade de actuação de um inimigo militar ou de forças não convencionais, numa determinada área de operações.

0615. O Ciclo de Targeting

A inter-relação das funções requeridas por uma força militar contra um objectivo é designada como Ciclo de *Targeting*. Na figura seguinte descreve-se os passos do referido ciclo.

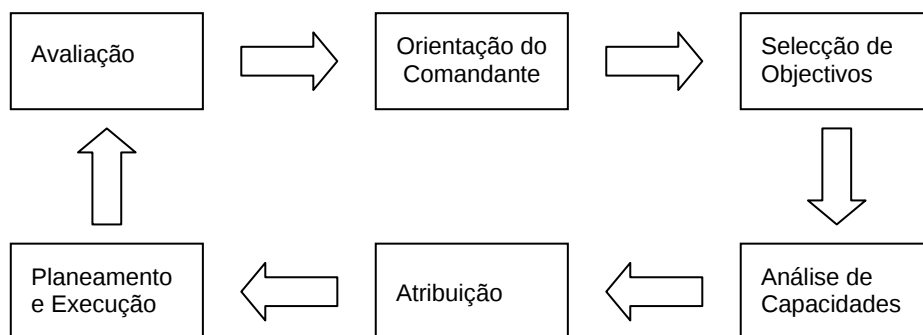


Figura 6-3 - O Ciclo de Targeting

0616. Targeting e o Plano de Campanha

O JFC estabelece um amplo quadro de objectivos para planeamento e difunde orientações para o ataque aos CoG estratégicos e operacionais e interdição das forças adversárias, como uma parte integrante da campanha e de operações de grande envergadura. Estes objectivos devem ser alcançáveis e mensuráveis para assegurar o progresso e avaliação da campanha. Aconselhado pelos comandos subordinados, o JFC estabelece prioridades, dá orientações no âmbito do *targeting* e determina o peso do esforço a ser desenvolvido durante as várias operações. Desta forma, os comandos subordinados recomendam ao JFC como utilizar o seu poder de combate de forma mais eficaz, tendo em vista alcançar os objectivos estabelecidos. O peso do esforço para qualquer aspecto relativo ao *targeting* conjunto pode ser expresso em termos de

PDE 2-00 Informações, Contra-Informação e Segurança

percentagem de recursos totais disponíveis, pelas prioridades atribuídas de recursos usados relativamente aos outros aspectos da campanha ou operação ou, ainda, como determinado pelo JFC.

0617. Targeting Conjunto – Resumo

O processo de *targeting* no nível operacional é crítico para o planeamento da campanha, pois o cuidado no ataque directo a objectivos chave poderá ter um impacto significativo no desfecho da mesma. A importância política e outros acontecimentos ligados ao *targeting* e a sua orientação e direcção deverão ficar retidos ao mais elevado nível. Por isso, quando as decisões relativas ao *targeting* permanecem nos níveis operacional e tático, devem enquadrar-se de acordo com a orientação e direcção estratégicas. A moderna tecnologia permite incrementar a eficácia com que as munições convencionais e não-letais podem ser utilizadas para atingir objectivos estratégicos e operacionais. Manter o controlo deste tipo de capacidades de forma a garantir que a sua aplicação decorrerá de acordo com os objectivos nacionais, aspirações estratégicas e com o plano de campanha, tem constituído um aspecto cada vez mais relevante. Além disso, a exploração destas capacidades tem inevitavelmente implicações políticas e presenciais. O resultado de tudo isto tem sido desenvolvido através do processo de *targeting*, mecanismo pelo qual os níveis político, estratégico e operacional controlam a aplicação do poder de fogo. Em resumo, este processo define que objectivos devem ser seleccionados, quais os meios que os irão atingir e por que ordem de prioridade. Especificam igualmente, quais os objectivos que são restritivos ou que não podem ser designados como tal.

0618. As Informações e Operações de Informação no nível Operacional

- a. Num QG conjunto, a Célula de Coordenação de INFO OPS Conjuntas (JIOCC - *Joint INFO OPS Coordination Cell*) deve ser estabelecida para planear e auxiliar na execução das INFO OPS. O chefe da Célula de Informações Conjunta (CJ2 – *Intelligence Joint Cell*) assume um papel chave nesta organização e as informações e contra-informação encontram-se igualmente representadas. Em termos gerais, a CJ2 é responsável por manter uma base de dados que permita avaliar as capacidades de INFO OPS do inimigo, suas vulnerabilidades e métodos.
- b. Muitas das capacidades de INFO OPS, particularmente as ofensivas, são incrementadas através de uma projecção antecipada. Neste sentido, o JIPB deve ser conduzido logo que possível para permitir:

- (1) O conhecimento das características técnicas dos sistemas de informação.
 - (2) O conhecimento dos factores políticos, sociais e culturais.
 - (3) As possíveis modalidades de acção das INFO OPS para os inimigos.
 - (4) Um entendimento do processo de decisão do inimigo.
 - (5) Uma perspectiva detalhada do processo de decisão político e militar do inimigo.
- c. Nas INFO OPS ofensivas, o *targeting* centra-se nos decisores e nas ligações estabelecidas entre eles. Os objectivos a designar podem incluir, entre outros: a capacidade de liderança do inimigo, infra-estruturas militares e civis e sistemas de armas. As informações apoiam este processo através da identificação dos decisores chave e de outros factores relacionados com o *targeting* que possam ter o máximo impacto sobre estes. As INFO OPS defensivas destinam-se a proteger o nosso processo de decisão, os nossos processos baseados em informações e os nossos SIC. Neste âmbito, as células de informações prestam o seu apoio através da identificação das ameaças (Indicações e Avisos - I&W – *Indications and Warning*) e da avaliação do risco.

0619. As Informações no apoio às Operações Pós-Conflito

Atingido o estado final militar, em qualquer operação ou campanha, deve verificar-se a transferência da responsabilidade da componente militar para a civil. Esta transferência deve ser incluída no planeamento estratégico e no da força conjunta. As informações podem apoiar a transferência de diversas formas, mas em primeiro lugar compete-lhes assegurar I&W sobre as ameaças à segurança e ao ambiente de transição.

SECÇÃO V – ARQUITECTURA CONJUNTA DAS INFORMAÇÕES

0620. Objectivo

- a. O JFC deve ser capaz de coordenar as acções das pessoas, organizações e recursos colocados à sua disposição a longas distâncias. O sucesso das operações requer que o JFC seja apoiado por uma infra-estrutura integrada de Comando, Controlo, Comunicações, Computadores e Informações (C4I), capaz de gerar e transmitir informação operacional e ordens, onde forem necessárias e no mais curto espaço de tempo possível.

PDE 2-00 Informações, Contra-Informação e Segurança

- b. Para se superiorizarem relativamente ao inimigo, os ciclos da decisão e da execução do JFC devem tornar-se mais consistentes que os dos opositores e capazes de garantir informações de maior qualidade. Ser mais rápido e melhor requer um efectivo controlo sobre a pesquisa, processamento e disseminação da informação.
- c. A estrutura C4I de apoio deve ser interoperável, flexível, móvel, disciplinada, sustentável e garantir capacidade de sobrevivência e de resposta. As organizações de informações utilizam diversos sensores e outras origens para pesquisar, analisar e produzir dados, fornecendo a interface de comunicações e de informação interna para transmitir informações.

0621. Características

A arquitectura operacional conjunta das informações deve assentar numa estrutura dinâmica e flexível, capaz de garantir o acesso global a uma informação em rede e baseia-se em todos os órgãos de informações nos diversos escalões.

A arquitectura está presente em cada fase do ciclo da produção da informação, desde o planeamento e direcção até à disseminação e integração, incluindo a supervisão e avaliação realizadas em todas as fases. Apoia as funções das informações sobre a rede de distribuição global, empregando para o efeito sistemas de comunicações, computadores, sistemas de apoio C4I baseados no espaço e seus recursos e tecnologias associados.

A arquitectura operacional apoia todo o espectro das operações militares, tal como previstas no OPP. Para esse fim, apoia as necessidades de informações do JFC e incorpora as orientações, procedimentos, pessoal treinado, sistemas de processamento automático de informação e a ligação para pesquisar, processar e disseminar informações que se encontram reunidas nos sistemas C4I do JFC.

0622. Considerações sobre o Planeamento

O planeamento da arquitectura conjunta de informações requer uma identificação atempada das necessidades de informação, incluindo parâmetros relativos a procedimentos e de âmbito técnico. O fluxo da informação, a oportunidade, o conteúdo, o formato e as prioridades são os factores fundamentais para a construção do modelo que melhor satisfaz as especificações técnicas de uma arquitectura de informações que mais eficientemente apoia um JFC. No âmbito da OTAN, os quatro domínios da arquitectura das informações descritos no Capítulo 5 devem constituir a base para o JFC.

O planeamento da arquitectura conjunta de informações deve assegurar a sobrevivência, segurança e interoperabilidade das arquitecturas de informações e a informação nelas contida, para satisfazer todas as combinações de configurações governamentais-comerciais. Factores organizacionais, doutrinários e de pessoal devem ser considerados igualmente para maximizar os benefícios das arquitecturas técnicas, tendo em vista atingir os fins do JFC.

0623. Necessidades

As células de informações que integram os EM das forças conjuntas são responsáveis por estabelecer a arquitectura operacional de informações necessária para o cumprimento da missão. Esta arquitectura deve satisfazer as necessidades de informação do JFC. Por outro lado, importa que as informações possam ser disponibilizadas para que possam ser rapidamente compreendidas e imediatamente utilizáveis; ou seja, já desprovidas de dados desnecessários.

A disseminação das informações consiste nos princípios de controlo *“push and pull”*, competindo à célula de informações o seu estabelecimento. O conceito *“push”* permite aos escalões mais elevados disponibilizarem informação aos subordinados, para satisfazer as suas necessidades ou para repor outra informação pertinente. O conceito de *“pull”* consiste no acesso directo a bases de dados, ficheiros de informações ou outros repositórios, pertencentes a órgãos de informações a todos os níveis. As actualizações *“push”* devem basear-se nas PIR do JFC, de forma a assegurar que lhe são fornecidas todas as informações críticas. Outra informação deve estar disponível, se necessária, numa base *“pull”*, de forma a evitar o excesso de informação.

A arquitectura operacional deve assegurar que nenhum órgão de pesquisa, produção ou disseminação é objecto de qualquer falha. Ao mesmo tempo, a arquitectura deve identificar e eliminar a desnecessária duplicação das capacidades de informações, tendo em atenção que os recursos são escassos e, como tal, devem ser focalizados para atingir as necessidades prioritárias.

A arquitectura operacional deve ser capaz de abranger o maior espectro possível de missões e de cenários operacionais. Para o efeito, deve responder às necessidades de informações do JFC em qualquer altura ou local e capaz de apoiar as operações multinacionais sem interrupções, de acordo com a fita de tempo estabelecida. Adicionalmente, deve permitir uma total integração dos ciclos da decisão e da execução do JFC em todas as fases do ciclo da produção da informação. No desenvolvimento da arquitectura operacional, a comunidade das informações deve agilizar o processo em

PDE 2-00 Informações, Contra-Informação e Segurança

cada fase do ciclo, de forma a garantir a capacidade de resposta às necessidades do JFC.

O desenvolvimento e implementação da arquitectura de informações operacional devem ser coordenados em estreita ligação com o SIC.

0624. Quartel-General da Força Tarefa Conjunta Combinada

Um QG CJTF é um quartel-general projectável, não permanente, multinacional, conjunto, de dimensão e composição variável, desenhado de acordo com a missão e tem por propósito auxiliar o Comandante (COMCJTF – *Commander of Combined Joint Task Force*) no exercício do C2 sobre toda a CJTF. É activado quando uma ordem é emanada directamente para exercer o C2 sobre forças multinacionais e conjuntas no prosseguimento de uma missão comum. A estrutura de um QG CJTF integra dois elementos: o EM do QG CJTF – responsável pelo planeamento e conduta das operações e o respectivo elemento de apoio. O primeiro é formado a partir de um núcleo de pessoal pré-identificado de um dos QG da estrutura de comandos da OTAN (*Parent HQ*) e aumentado com pessoal e equipamento para atingir e manter uma total capacidade operacional. Em cada QG da estrutura de comandos da OTAN deve existir, em permanência, uma Força Tarefa Conjunta Projectável (DJTF - *Deployable Joint Task Force*) que será aumentada posteriormente, para formar um QG Operacional, totalmente estruturado para o cumprimento da missão. Um modelo genérico de um QG CJTF é o que se apresenta na figura seguinte.

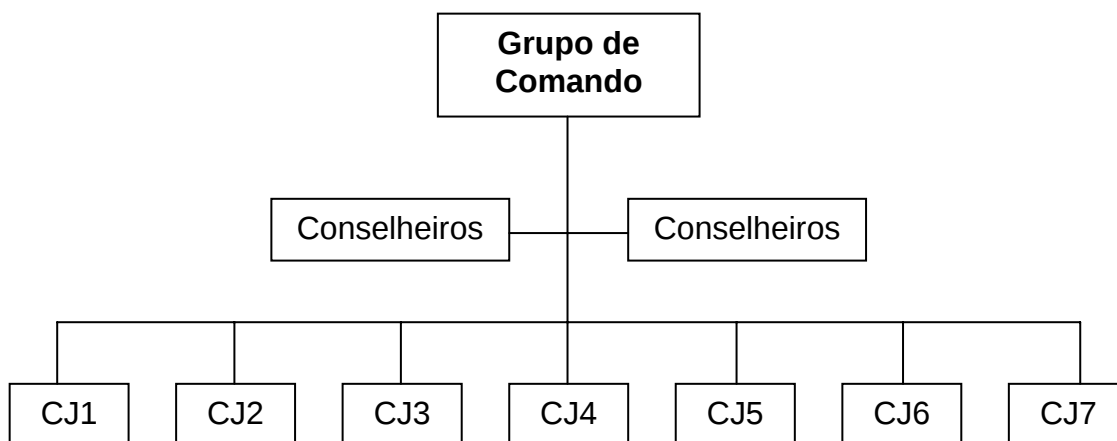


Figura 6-4 – Modelo Genérico da Estrutura de um QG CJTF

O modelo genérico de uma estrutura de um QG CJTF inclui a Célula de Informações que apresenta a seguinte organização:

REPARTIÇÃO	SECÇÃO
SEC I <i>Executiva</i>	CJ2
	Apoio Administrativo / Processamento Automático de Dados
SEC II <i>Planos</i>	Chefe
	Planos
SEC III <i>Operações</i>	Chefe
	Operações Correntes e Avaliação
	Bases de Dados
	SIGINT
	Geográfica e Análise de Terreno
	CCIRM
	Targeting
	Reconhecimento e Ligação
SEC IV <i>HUMINT, Contra- Informação e Segurança</i>	Chefe
	Contra-Informação
	Segurança
	HUMINT

0625. Apoio das Informações

As CJTF necessitarão de conceber uma estrutura de informações numa base ampla para abranger um espectro alargado de opções. O carácter variado e imprevisível das missões CJTF, e por consequência, do apoio das informações, necessitará de estruturas flexíveis e adaptáveis baseadas em princípios acordados e em procedimentos estabelecidos. A disponibilidade e extensão do apoio das informações da OTAN a CJTF lideradas pela União Europeia (UE) e a operações que podem integrar nações não-OTAN, deverá ser solicitado o mais cedo possível durante a fase de planeamento e, subsequentemente, durante a conduta das operações quando necessário.

0626. Condições

A disponibilidade de informações consolidadas e avaliações que cobrem o domínio político, social, económico, militar e de informação, são imprescindíveis para garantir um alerta estratégico oportuno e possibilitar a preparação e geração das forças necessárias, bem como das respectivas capacidades.

0627. Princípios

As intenções e necessidades de informação de uma CJTF devem constituir o guia fundamental dos esforços das informações. Estas determinam as necessidades específicas de informações e a organização e gestão da informação para as operações específicas definidas pelo COMCJTF. A garantia de informações efectivas deve nortear-se pelos seguintes princípios:

- a. A comunidade de informações da OTAN e todas as nações participantes garantem apoio de informações às missões CJTF.
- b. O QG CJTF necessita de ser apoiado por uma organização de informações capaz, gerada durante o processo de activação da força.
- c. Para garantir a máxima eficiência e efectividade das operações CJTF, as arquitecturas de informações, tecnologias, estrutura e doutrina devem ser harmonizadas com as forças, necessidades e capacidades.
- d. Contribuições de elevada qualidade e atempadas por parte das nações constituem elementos críticos. Numa crise emergente, a CJTF deve dispor, o mais cedo possível, de meios e capacidades de reconhecimento e de informações para poder complementar as contribuições de informações cedidas pelas nações.
- e. A Contra-Informação constituirá uma importante necessidade ao assegurar a efectividade das operações.

0628. Centro de Informações Conjunto

O Centro de Informações Conjunto (JIC – *Joint Intelligence Centre*) é a organização primariamente responsável por garantir apoio ao QG CJTF. O seu conceito assenta na fusão das principais capacidades de apoio de todas as componentes e das unidades de

combate até uma localização central para o apoio das informações. Embora se espere que não seja capaz de satisfazer completamente todos os RFI pode no entanto, coordenar o apoio de outras organizações de informações, de escalões inferiores, superiores ou laterais.

O JIC deve ser desenhado de forma flexível e pode expandir-se de forma a alcançar as necessidades do JFC. Durante os períodos de paz e estabilidade, os níveis de pessoal do JIC manter-se-ão no nível mínimo exigido para garantir as funções essenciais, tais como: I&W, informações correntes, gestão da pesquisa e outras responsabilidades genéricas de produção de informações militares na área do JIC.

0629. Células Nacionais de Informações

Apesar do COMCJTF poder estruturar o QG CJTF, desde que considere apropriado, o seu EM pode integrar representantes das informações de nações participantes e de outros serviços, sob a forma de contribuições de pessoal nacional. Adicionalmente, um determinado número de NIC serão normalmente incluídos no QG CJTF, numa base de voluntariado, para servirem como elo de ligação entre os departamentos governamentais de informações e a célula de informações do QG CJTF.

Página intencionalmente em branco

CAPÍTULO 7 NÍVEL TÁCTICO DAS OPERAÇÕES

SECÇÃO I – GENERALIDADES

0701. Introdução

A finalidade deste capítulo é descrever os procedimentos das informações e sua aplicação ao nível táctico.

0702. Nível Táctico

Os níveis das informações estão ligados aos objectivos das operações e não necessariamente a escalões específicos. Ao nível táctico, as informações apoiam o combate e outros empenhamentos. As informações tácticas são caracterizadas pela rápida deterioração e capacidade para de imediato influenciar o resultado da missão.

a. Operações terrestres ao nível táctico

No contexto das operações terrestres, as informações tácticas apoiam normalmente a componente e os escalões mais baixos.

b. Operações navais ao nível táctico

Ao nível táctico, as operações navais englobam os grupos-tarefa (*task groups*), os quais conduzem operações no âmbito de uma operação conjunta.

c. Operações aéreas ao nível táctico

Embora as operações aéreas estejam focalizadas ao nível operacional, os meios de reconhecimento e vigilância podem ser usados para obter a informação necessária aos três níveis da guerra. As informações apoiam o emprego das unidades, treino de prontidão e planeamento. A maior parte das unidades de informações são compostas de duas valências – informações operacionais (também designadas de combate) e informações de objectivos. Cada uma desenvolve uma missão específica.

(1) Informações operacionais

As informações operacionais mantêm o comandante e as guarnições informadas sobre os assuntos das informações necessárias para o cumprimento da missão. Mantêm os dados actualizados, executam briefings e treinos, auxiliando o planeamento da missão.

PDE 2-00 Informações, Contra-Informação e Segurança

(2) Informações de objectivos

Reúnem e mantêm os ficheiros actualizados acerca da documentação sobre os objectivos.

0703. O Papel das Informações ao Nível Tático

O grande contributo das informações para o comandante é serem a base para a Imagem Operacional Comum (COP – *Common Operational Picture*). Inclui o conhecimento do dispositivo, capacidades e possíveis intenções do inimigo, bem como os factores físicos, meteorológicos e socio-económicos que moldam o ambiente do espaço de batalha. Desta forma permite ao comandante empregar as suas funções de combate contra as forças inimigas para atingir os objectivos de nível operacional.

0704. A Importância das Informações ao Nível Tático

a. Abordagem “Todas as Origens”

É muito importante que os meios de aquisição sejam empregues de modo a garantir uma imagem compreensiva e precisa acerca do espaço de batalha.

As informações são processadas a partir de informação obtida através de origens independentes. Depender de uma só origem de informação deve ser a excepção, pelo que a integração de todos os meios disponíveis é fundamental na produção de informações. Uma Célula de Todas as Origens (ASC – *All Source Cell*) é, por conseguinte, a chave para integrar essas origens.

b. Factores

(1) Tempo

O tempo é o elemento crítico para orientar o esforço de pesquisa, pesquisar, processar e disseminar as informações.

(2) Recursos

A disponibilidade de meios e de pessoal para pesquisar é fundamental para satisfazer as necessidades de informações do comandante.

0705. Dimensões

As informações devem considerar o espaço de batalha em termos de espaço e tempo. O espaço de batalha é visto como tendo três dimensões – altitude, profundidade e largura – e engloba o ambiente humano, de informação e electromagnético. O combate em profundidade, próximo e na área da retaguarda deve ser considerado a todos os

níveis. Estes factores determinam a Área de Responsabilidade de Informações (AIR – *Area of Intelligence Responsibility*) e a Área de Interesse (AOI – *Area of Interest*).

0706. O Papel do Estado-Maior

Ao nível tático, os elementos chave no processo das informações são o Comandante, o Oficial de Informações¹⁶ e o Oficial de Operações¹⁷.

a. Comandante

Além de dirigir as operações, o comandante dirige também o processo de obtenção de informação em apoio às operações. Por outras palavras, o comandante dirige as informações. Os especialistas em informações apoiam o comandante através de um trabalho detalhado de Estado-Maior (EM) para tirar o máximo rendimento dos meios ao seu dispor. O comandante, ao estabelecer as Necessidades de Informação Crítica do Comandante (CCIR – *Commander's Critical Information Requirements*), identifica as Necessidades Prioritárias de Informações (PIR – *Priority Intelligence Requirements*) relacionadas com o inimigo, terreno e condições meteorológicas. Para assegurar que os PIR são relevantes, estes são comunicados pelo comandante ao seu EM, aos comandantes subordinados e a outras células de informações. O comandante define quando é que a informação relacionada com os PIR deve ser fornecida. O tempo é um factor crítico, dado que tem influência nas tarefas a atribuir aos órgãos de pesquisa, bem como nos processos de disseminação a utilizar. O comandante deve, também, assegurar-se que:

- (1) Os meios de pesquisa orgânicos são suficientes e estão atribuídos ao processo de pesquisa.
- (2) O esforço das células de informações e operações está sincronizado de modo a funcionar em conjunto como uma equipa coesa.

b. Oficial de Informações

O oficial de informações é o oficial de EM que primariamente está vocacionado para as operações futuras do inimigo e para o efeito que o ambiente tem nas operações das forças amigas e do inimigo. É o oficial primariamente responsável pelo ciclo da

¹⁶ G2 – Escalão Divisão e em alguns países escalão Brigada.

S2 – Escalão Brigada e Batalhão

Os equivalentes nas componentes naval e aérea são, respectivamente, N2 e A2

¹⁷ G3 – Escalão Divisão e em alguns países escalão Brigada.

S3 – Escalão Brigada e Batalhão

Os equivalentes nas componentes naval e aérea são, respectivamente, N3 e A3

Os equivalentes nas componentes naval e aérea são, respectivamente, N3 e A3

PDE 2-00 Informações, Contra-Informação e Segurança

produção da informação e pelo adequado apoio de informações ao comandante. Assim, o oficial de informações auxilia o comandante no entendimento do espaço de batalha e da operação, na perspectiva do comandante inimigo. Após receber as directivas do comandante, o oficial de informações emite a sua directiva para a célula de informações para assegurar a convergência de esforços para a operação. O oficial de informações também determina e desenvolve as necessidades de informação e indicadores que são a base do plano de pesquisa.

c. Oficial de Operações

O oficial de operações é o oficial primariamente responsável pela capacidade de combate da unidade e pela sua prontidão. Pode desempenhar um papel fundamental na orientação do esforço de pesquisa, em particular:

- (1) Participa na formulação de PIR e na determinação de necessidades de informação.
- (2) Fornece necessidades de informação adicionais ao oficial de informações, a serem incluídas no plano de pesquisa.
- (3) Emite ordens de pesquisa aos órgãos de pesquisa que não estão inseridos na estrutura das informações. O envolvimento do oficial de operações neste processo garante o necessário controlo centralizado sobre todos os órgãos de pesquisa e assegura a economia de esforço.

SECÇÃO II – AS INFORMAÇÕES E O PROCESSO DE DECISÃO MILITAR

0707. Generalidades

O comandante e o seu EM utilizam o Processo de Decisão Militar (PDM) para seleccionar uma m/a e desenvolver planos ou ordens para a implementar. O oficial de informações, como elemento preponderante no processo, garante as notícias e informações necessárias acerca do inimigo e ambiente operacional. A figura 7-1 ilustra a relação entre o Estudo do Espaço de Batalha pelas Informações (IPB – *Intelligence Preparation of Battlefield*), o Ciclo da Produção da Informação e o PDM.

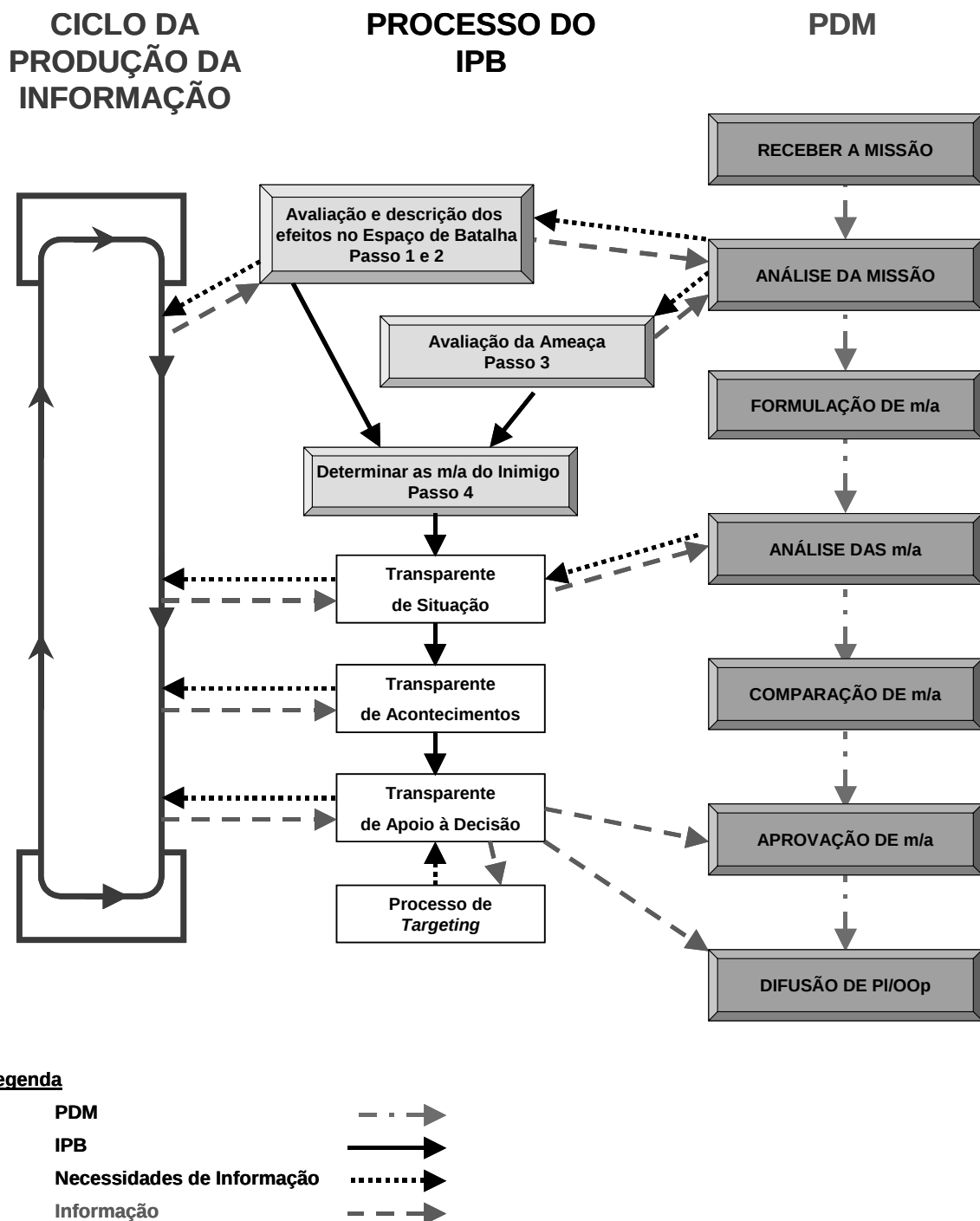


Figura 7-1 – Relação entre o Ciclo da Produção da Informação, o IPB e o PDM

0708. As Responsabilidades e Tarefas do Oficial de Informações durante o PDM (A leitura deste parágrafo deve ser complementada com a leitura do Anexo A - AS RESPONSABILIDADES E TAREFAS DO OFICIAL DE INFORMAÇÕES DURANTE O PDM)

O oficial de informações é o responsável pelas seguintes tarefas durante o PDM:

a. Fase 1 – Recepção da Missão

O PDM inicia-se com a antecipação ou recepção de uma nova missão, ou ainda com uma alteração significativa da situação, que indica ao comandante que poderá ter a oportunidade de cumprir a missão com a adopção de uma m/a significativamente diferente da anteriormente implementada.

b. Fase 2 – Análise da Missão

Após a recepção da ordem do escalão superior, o comandante vai determinar o que a unidade terá de executar. O comandante e o EM asseguram-se que foi cabalmente assimilada a intenção, a missão, o conceito de operação e a fita do tempo do escalão superior, bem como das unidades adjacentes. Deste modo, o oficial de informações elabora os seguintes produtos:

(1) Estudo da Situação de Informações

O estudo da situação de informações pode ser melhorado ou substituído pelos produtos do IPB. Para poupar tempo, o oficial de informações deve utilizar, se possível, os produtos fornecidos pelo escalão superior.

(2) Transparente de Obstáculos Combinados Modificado (TOC-M)

A partir dos produtos fornecidos pelo escalão superior, o oficial de informações deve, o mais rapidamente possível, desenvolver o próprio TOC-M com toda a informação essencial acerca dos aspectos militares do terreno. Baseado no conhecimento do inimigo e da representação gráfica do TOC-M, possíveis m/a devem ser de imediato identificadas.

(3) Lista de Objectivos de Elevado Valor (HVTL)

De acordo com as m/a, deve ser preparada uma HVTL.

(4) Lista de PIR

O oficial de informações deve ter disponível uma lista de PIR para o comandante. Durante a análise da missão, o comandante e EM formulam CCIR e os PIR. Outros oficiais do EM identificam falhas nas informações

disponíveis e contribuem para a formulação de PIR e determinação de outras necessidades de informação.

Baseado no estudo da situação de informações e no IPB, o comandante emite as directivas para focalizar as actividades de EM no planeamento da operação. O oficial de informações deve ter uma ideia clara acerca das m/a do inimigo a considerar, bem como o estabelecimento da sua probabilidade de ocorrência, as CCIR, de como devem ser focalizados os meios Informações, Vigilância, Aquisição de Objectivos e Reconhecimento (ISTAR – Intelligence, Surveillance, Target Acquisition and Reconnaissance), das medidas de segurança a implementar e da fita do tempo para planeamento e execução da operação.

c. Fase 3, 4 e 5 – Formulação, análise e comparação das modalidades de acção (M/A)

Baseado no IPB inicial e necessidades de informação identificadas durante a análise da missão, o oficial de informações desenvolve o plano de pesquisa para obter as informações necessárias. O plano de pesquisa será refinado constantemente durante o processo de planeamento e durante a execução da operação. Para apoiar o desenvolvimento das m/a, o oficial de informações apoia o oficial de operações na análise do potencial relativo de combate (PRC), que inclui os ratios de força e a identificação dos pontos fortes e fracos do inimigo.

Na preparação para a análise, as M/A do inimigo são desenvolvidas a partir da integração e refinamento dos produtos do IPB. Para cada m/a do inimigo é elaborado um transparente de situação de acordo com as suas tácticas, equipamentos e influência do ambiente operacional. Estes transparentes são utilizados para o jogo da guerra durante a análise das M/A.

O jogo da guerra testa a nossa M/A contra as m/a do inimigo, de modo a identificar a m/a que tem mais vantagens, especialmente aquela que tem menos riscos e que melhor posiciona a unidade para a acção ulterior. Durante o jogo da guerra é melhorado também o transparente de acontecimentos, no qual são identificadas as áreas designadas de interesse (NAI – Named Area of Interest), nas quais é possível identificar os indicadores de m/a do inimigo. Durante o jogo da guerra são também identificados os alvos remuneradores (HPT – High-payoff Targets) para a operação.

d. Fase 6 – Decisão

Baseado nos resultados do jogo da guerra, o comandante decide qual a m/a que melhor pode cumprir a missão com mais vantagens.

e. Fase 7 – Difusão de Planos e Ordens de Operações

Os oficiais de informações, operações e representantes das funções de combate desenvolvem o transparente de apoio à decisão para facilitar o processo de targeting e apoiar o comandante a monitorizar o combate. As áreas com objectivos de interesse (TAI – Targets Areas of Interest), são áreas onde o comandante pode influenciar o combate através da destruição, retardamento e desorganização das forças adversárias. Neste transparente são graficados os pontos de decisão e os TAI, que por sua vez devem ser incluídos no plano de ISTAR.

- f.** No decurso da operação, o oficial de informações deve assegurar-se que o comandante e o EM estão sempre informados acerca da situação do inimigo. Como o oficial de informações é determinante para que o comandante tenha um conhecimento actualizado da situação, deve continuamente refinar os produtos do seu IPB e divulgá-los.

SECÇÃO III – TARGETING**0709. Generalidades**

O ciclo do *Targeting* baseia-se no ciclo das funções de: Decidir, Detectar/Seguir, Executar e Avaliar. Esta metodologia proporciona uma análise sistemática que permite produzir os efeitos desejados sobre o objectivo pretendido, com o sistema de armas mais adequado e no momento e local oportunos. O processo, apresentado graficamente na figura 7-2, constitui um método eficaz de adequação das capacidades das Forças Amigas aos objectivos mais importantes, permitindo ao comandante da força obter os efeitos desejados. É um processo dinâmico que permite às entidades nele envolvidas adaptarem-se às rápidas alterações da situação. Esta metodologia, bem como as suas ferramentas e produtos, devem ser continuamente revistos à medida que a situação evolui e actualizados com base nos relatórios de situação e avaliações do combate. As

funções não são necessariamente faseadas ou sequenciais, podendo frequentemente surgir durante o planeamento e/ou a execução operacional.

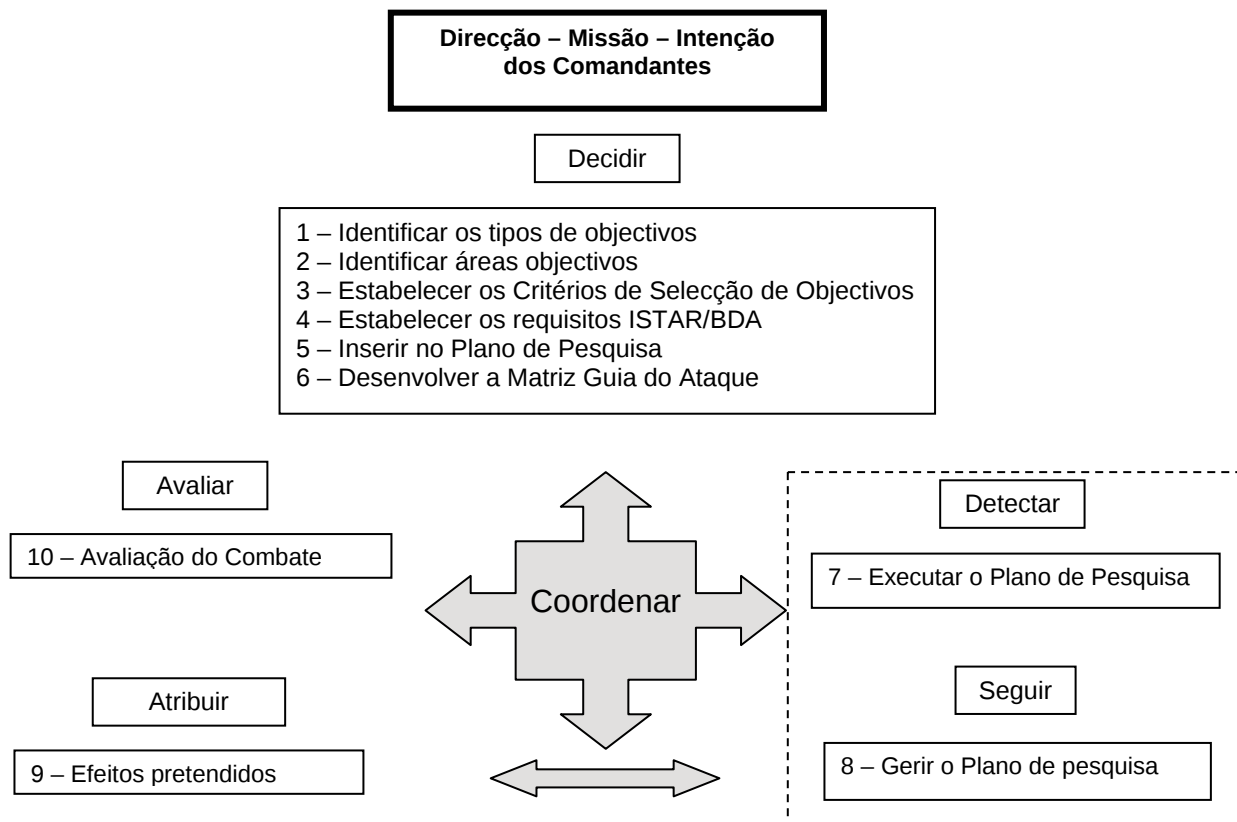


Figura 7-2 Ciclo de Targeting

0710. Função Decidir

Esta é a função inicial e aquela que envolve um maior número de elementos do EM. A eficácia do esforço do EM durante esta fase do ciclo irá determinar provavelmente a eficácia de todo o ciclo de *Targeting*. O *Targeting* desenvolve-se em simultâneo e em paralelo com o esforço de recolha de informações e estudos realizados pelo EM, podendo auxiliar na definição de prioridades na recolha de informações e no planeamento dos efeitos pretendidos.

Esta função divide-se em 6 sub fases:

a. Identificar o tipo de Objectivos

O tipo e a categoria de objectivos dependem da natureza da operação e dos efeitos que se pretendem obter. Os objectivos são introduzidos em listas que irão sendo actualizadas perante a recolha de informações e a evolução das necessidades/requisitos estabelecidos pelos Comandantes.

b. Identificar áreas objectivo

Esta fase apenas envolve a Área de Operações (AOO – *Area of Operations*) e identifica as áreas de interesse para o *Targeting*. Devem ser tidas em consideração todas as dimensões do espaço de batalha e as possíveis limitações, designadamente as áreas protegidas.

c. Estabelecer os Critérios de Selecção de Objectivos (TSS – *Target Selection Standards*)

As capacidades de detecção e de ataque disponíveis ditarão os limites técnicos e os procedimentos a estabelecer. É importante associar os meios adequados, de ISTAR e de ataque (letais ou não-letais), ao tipo de objectivo a adquirir e a atacar.

d. Inserir no Plano de Pesquisa

A inserção dos requisitos do Targeting no Plano de Pesquisa tem por finalidade a gestão dos sistemas de detecção. Esta integração conduz à identificação dos objectivos prioritários, como poderão ser detectados e se é necessário seguir os mesmos.

e. Estabelecer os requisitos ISTAR/BDA

A tomada de decisão deve ocorrer o mais cedo possível para se obter sucesso no ataque. Na tomada de decisão, devem igualmente ser consideradas aquelas que dizem respeito à orientação dos sistemas para garantir uma avaliação de danos (BDA – *Battle Damage Assessment*) eficaz. Apenas uma BDA eficaz garante que os efeitos pretendidos pelo Comandante são alcançados.

f. Desenvolver a Matriz Guia do Ataque (AGM – *Attack Guidance Matrix*)

A AGM, produto final e consolidado desta fase, serve de apoio às decisões de *Targeting*. Constitui um documento prático que proporciona rapidez nas decisões de ataque durante o desenrolar das operações. Deve ser desenvolvida uma AGM para cada operação e para cada fase da operação, quando esta é faseada.

0711. Designação de Objectivos**a. Transferência de Objectivos para escalões superiores**

Quando as capacidades requeridas para bater um objectivo ou cumprir uma missão ultrapassam as da força, este/a deve ser transferido/a para o escalão imediatamente superior, pelo que o EM deve ser capaz de identificar quando um

objectivo deve ser atribuído ao ciclo de *Targeting* do escalão superior. Para garantir a necessária coordenação, no planeamento e na execução, é aconselhável a troca de Oficiais de ligação entre Comandos.

b. Objectivos atribuídos pelos escalões superiores

Os Objectivos atribuídos pelo escalão superior devem ser integrados no ciclo de *Targeting*, sendo-lhes atribuída uma prioridade de acordo com as directivas do Comandante. A atribuição de objectivos a uma Unidade, pelo seu escalão superior, poderá limitar a disponibilidade de meios de detecção, de seguimento e de ataque necessários à consecução dos objectivos estabelecidos pelo Comandante.

0712. Produtos da Função Decidir

As finalidades da função Decidir são a unidade do esforço no processo *Targeting* e um conjunto de produtos de apoio. A seguir, indicam-se alguns dos produtos resultantes desta fase:

a. HVTL

A HVTL resulta de considerações sobre a missão, das intenções e das vulnerabilidades do inimigo e da directiva do Comandante. Esta lista é geralmente elaborada pela célula de informações. Os HVT constituem as capacidades/estruturas cuja perda degrada seriamente a capacidade do inimigo para atingir os seus objectivos. Por defeito, e conforme requerido pelo Sistema Automático de Comando e Controlo (AFATDS – Advanced Field Artillery Tactical Data System), as categorias de objectivos são as seguintes:

Nº	Designação
1	Comando e Controlo
2	Apoio de Fogos
3	Manobra
4	Defesa Aérea
5	Engenharia
6	Informações, Vigilância, Aquisição de Objectivos e Reconhecimento (ISTAR)
7	Guerra Electrónica
8	NBQ
9	Classe III (combustíveis)

10	Classe V (munições)
11	Classe IX (sobressalentes)
12	Transporte
13	Linhas de comunicação

b. HPTL

A HPTL constitui uma decisão do Comandante, que deve ser difundida em conformidade. Esta lista contém os HVT cuja destruição ou neutralização contribui significativamente para o sucesso da operação e que podem ser atingidos pelos sistemas disponíveis da força considerada. A HPTL pode ser utilizada para orientar o esforço de pesquisa, devendo ser alterada de acordo com a fase e natureza das operações. No Anexo B apresenta-se um exemplo de HPTL.

c. TSS

Os TSS são critérios a aplicar a possíveis objectivos futuros para determinar quais os sistemas de detecção que, pelo seu grau de precisão e tempo de resposta, permitem o emprego eficaz do sistema de armas seleccionado para a execução do ataque. No anexo B apresenta-se um exemplo de matriz dos TSS.

d. AGM

A AGM especifica o método de ataque aos HPT; quando e como deverão ser atacados e restrições ao ataque. Facilita o planeamento táctico e o logístico ao designar o meio de ataque para cada objectivo. No anexo B apresenta-se um exemplo de AGM.

e. BDA

Os objectivos que requerem uma BDA são identificados e transmitidos para a célula de informações. Este assunto irá ser abordado mais à frente na função Avaliar.

f. Tabela Conjunta de HPT/TSS/AGM

Poderá ser útil combinar os produtos da função decidir. No entanto deve-se desenvolver separadamente os produtos para facilitar a verificação. No anexo B apresenta-se um exemplo.

Todos estes produtos devem ser expostos ao Comandante e aprovados por este ou pela entidade designada para a função de controlar e coordenar o esforço de *Targeting*.

0713. Definição de Objectivos

As informações desempenham um importante papel neste passo. A directiva do comandante e o IPB inicial ou estudo de situação de informações são a base para a produção de uma lista de HVT. Os HVT são os meios de importância crítica para que o inimigo atinja os objectivos nas suas operações. Ao nível tático os HVT podem incluir:

a. Geral

- (1) C4I.
- (2) Meios ISTAR.
- (3) Linhas de comunicações.
- (4) Armas de destruição maciça.
- (5) Logística.

b. Operações Terrestres

- (1) Quartéis-generais e postos de comando.
- (2) Unidades de manobra.
- (3) Reservas.
- (4) Artilharia e mísseis.
- (5) Meios de engenharia.
- (6) Helicópteros de ataque.

c. Operações Navais

- (1) Unidades de comando e controlo.
- (2) Unidades de combate de superfície.
- (3) Meios de aviação naval.
- (4) Meios de guerra anti-submarina.

d. Operações Aéreas

- (1) Meios de detecção e alerta.
- (2) Bases.
- (3) Meios de defesa aérea.
- (4) Meios de reabastecimento em voo.

0714. Função Detectar

A aplicação prática desta função consiste na execução do Plano de Pesquisa, cabendo à célula de informações a coordenação e execução de toda a actividade dos meios de pesquisa/detecção.

É essencial que todos os meios de detecção disponíveis (orgânicos, atribuídos e quando apropriado os meios do escalão superior, escalões subordinados, unidades adjacentes e unidades de outros ramos) sejam empregues de forma eficaz e eficiente, para tal:

- a. Deve ser proporcionado aos sistemas de detecção a informação sobre os Objectivos a detectar de forma clara e concisa.
- b. Deve-se evitar a duplicação de esforços na pesquisa, excepto quando se pretende confirmar a informação sobre os objectivos.
- c. Deve-se evitar vazios no esforço de pesquisa de informações.
- d. Os HPT devem ser detectados com precisão e atempadamente.

A informação obtida pelos sistemas de detecção é transmitida ao respectivo QG, e este por sua vez retransmite-a para o órgão que as requereu.

Enquanto que alguns dos sistemas de detecção produzem objectivos por si só, outros requerem que os dados obtidos sejam processados para que os objectivos sejam produzidos. As prioridades de *Targeting*, desenvolvidas durante a fase da Decisão, são utilizadas para abreviar o processamento dos dados sobre objectivos.

A informação obtida nesta fase é usada para actualizar e corrigir a HPTL e a AGM.

0715. Função Seguir

Esta função complementa a função detectar; no entanto distingue-se desta visto que o seguimento de um Objectivo requer uma gestão específica da decisão. Muitas destas decisões tácticas são acordadas durante a fase Decidir e integradas na AGM. Uma vez detectado, o HPT não é imediatamente atacado, contudo é seguido de modo a assegurar o conhecimento permanente da sua localização, para ser atacado posteriormente ou para ser validado. A Célula de *Targeting* tem de ter em atenção que um sistema, enquanto usado no seguimento, normalmente, não pode ser empregue para outra finalidade.

A gestão do plano de pesquisa, pela Célula de *Targeting*, tem por finalidade evitar que, durante o processo de pesquisa, se percam os objectivos antes de se consumir o ataque.

A necessidade de passagem de seguimento de objectivos entre sensores implica a necessidade da existência de requisitos para a sua gestão. Quanto maior for o número de sensores disponíveis maiores são as dificuldades de gerir a passagem de seguimento de Objectivos.

0716. Relatórios

À medida que a pesquisa é executada e a informação é recebida, esta vai sendo enviada para as fases mais apropriadas do ciclo *Targeting* para análise. Por isso, é essencial que os relatórios estejam completos.

0717. Função Atribuir

a. Generalidades

A actividade principal desta fase é produzir o efeito adequado sobre determinado Objectivo, de acordo com o registo da AGM. Associar efeitos letais a objectivos convencionais poderá ser relativamente fácil, contudo a gestão dos efeitos não-letais sobre objectivos de Operações de Resposta a Crises (CRO – *Crisis Response Operations*) poderá demonstrar-se mais difícil.

b. Durante a operação poderão surgir objectivos de oportunidade, objectivos importantes não planeados, que deverão ser processados do mesmo modo que os HPT. Estes, não incluídos na HPTL planeada, devem em primeiro lugar ser sujeitos a uma análise para determinar se e quando devem ser atacados. A decisão para atacar um objectivo de oportunidade apoia-se num conjunto de factores, tais como a actividade do Objectivo e a sua importância para a operação, quando comparados com os que estão a ser processados para ataque.

c. A decisão tática final de ataque obtém-se com a confirmação da selecção do sistema de efeitos (sistema que realizará o ataque) mais apropriado para cada objectivo, de acordo com a AGM.

d. A selecção do sistema de efeitos apropriado para Objectivos planeados é realizada durante a fase de Decidir. Não obstante, é necessário verificar se os sistemas

PDE 2-00 Informações, Contra-Informação e Segurança

requeridos existem e se estes podem executar o ataque. Caso contrário, a Célula de *Targeting* deve determinar qual é o sistema disponível mais adequado para executar esse ataque. Em alguns casos poderão ser empregues mais do que um sistema para atacar o mesmo objectivo.

- e. Uma vez tomadas as decisões tácticas, os órgãos apropriados enviam as ordens de execução aos sistemas designados. O Comandante do sistema de ataque verifica se tem ou não capacidade para executar a ordem de ataque e, em caso afirmativo, executa-o. Se por algum motivo não satisfaz os requisitos necessários para cumprir a ordem deve informar o respectivo órgão de comando. A Célula de *Targeting* reavalia a situação, analisa e verifica novamente os requisitos necessários para o cumprimento da ordem ou reencaminha a mesma para outro sistema que a possa executar.

0718. Função Avaliar

- a. A avaliação é o passo final do ciclo e tem como finalidade determinar a eficácia dos ataques sobre os objectivos seleccionados. A avaliação deverá ser um processo dinâmico e deverá estar sob constante atenção da Célula de *Targeting*.
- b. Um dos métodos de avaliação é designado por Avaliação do Combate (*Combat Assessment*) que inclui a BDA, a Análise da Eficácia das Munições (MEA – *Munitions Effectiveness Analysis*) e recomendações para bater novamente os Objectivos.
- c. A BDA é a avaliação atempada e precisa dos danos resultantes do emprego de efeitos letais e não-letais sobre um objectivo.

A necessidade de BDA para HPT específicos é determinada durante a fase Decidir, em que as necessidades de BDA são registadas na AGM e no Plano de Pesquisa.

A BDA é da responsabilidade da Célula de Informações. Os Comandantes e respectivos EM devem ter sempre em atenção que os recursos empenhados na BDA deixam de estar disponíveis para outras aquisições ou seguimentos de objectivos, pelo que devem ser estabelecidas e aprovadas prioridades de emprego para cada tipo de sistema de detecção. Os resultados da BDA são processados para determinar se os efeitos pretendidos sobre os Objectivos foram alcançados. Uma BDA eficaz implica o seguinte:

- (1) A nível tático, permite ao Comandante formar uma visão sobre os efeitos que as operações correntes têm no inimigo. Fornece uma estimativa sobre a eficácia para o combate e as capacidades residuais do inimigo.
 - (2) Como parte integrante no processo de *Targeting*, a BDA ajuda a determinar se são necessários novos ataques sobre os objectivos. Os Comandantes usam esta informação para atribuir ou redireccionar os sistemas de ataque com vista a obter o máximo rendimento do poder de combate ao seu dispor.
- d. A MEA, que consiste numa avaliação da eficácia do sistema de ataque seleccionados, é geralmente da responsabilidade da célula de Operações.
- e. A combinação da MEA com a BDA permitirá ao EM obter a informação necessária para aconselhar o Comandante. A eficácia, ou não, de um determinado ataque poderá exigir ter em consideração outras opções de ataque ou exigir que um Comandante altere determinados aspectos do seu plano para fazer face à situação emergente.

SECÇÃO IV – O CICLO DA PRODUÇÃO DA INFORMAÇÃO

0719. Passos

Ao nível tático, o Ciclo da Produção da Informação, detalhado anteriormente no Capítulo 3, consiste nos seguintes passos:

- a. **Orientação do Esforço de Pesquisa** – Determinar as informações necessárias e quem é que as vai obter.
- b. **Pesquisa** – Obter notícias de combate, informações e notícias de objectivos através de órgãos de pesquisa.
- c. **Processamento** – Através da análise das notícias de combate, produzir informações e estabelecer objectivos, determinando os que se adequam à situação.
- d. **Disseminação** – Transmitir informações e objectivos aos utilizadores quando deles necessitam.

0720. Finalidade do Ciclo da Produção da Informação

A finalidade do Ciclo da Produção da Informação é produzir informações para:

a. Avaliação da Situação

É a compreensão do ambiente operacional no contexto da missão. A célula de informações contribui para o conhecimento da situação descrevendo localizações, efectivos, tipos, direcções e ritmos de movimento, assim como actividades das forças adversárias. Contribuem para a compreensão do espaço de batalha pelo comandante através da descrição do terreno, condições meteorológicas, demografia, etc. com o detalhe suficiente para empregar de forma eficiente as forças e os sistemas de armas.

b. Desenvolvimento de Objectivos

É o processo de produção atempada e de localizações precisas de HPT do inimigo, como por exemplo: meios ISTAR, formações blindadas, instalações de comunicações tácticas, concentrações de artilharia, postos de comando, instalações vitais de sustentação. Com essa informação, os objectivos podem ser eficazmente atacados por fogos, manobra ou meios de guerra electrónica.

0721. Orientação do Esforço de Pesquisa

Durante esta fase:

- As informações e as necessidades de informação são determinadas com base nas CCIR e outras directivas do comandante à célula de informações.
- Às origens e órgãos (meios ISTAR) são atribuídas tarefas para obter informação.
- Deve ser continuamente verificada a produtividade das origens e órgãos.

a. Planeamento das Informações

Em conjugação com o IPB e PDM, a célula de informações prepara os seguintes produtos:

- **Plano de Pesquisa (Anexo C).**
- **Anexo de Informações (Anexo F).**

O anexo de informações é um anexo à ordem de operações, no qual a célula de informações apresenta as necessidades de informações.

- **Transparente ISTAR.**

Ilustra a cobertura de unidades ou meios ISTAR e constitui um apêndice ao anexo de informações.

- b. Monitorização**

Durante o combate, os comandantes necessitam de novas notícias e informações para o ajustamento nas operações correntes e para o planeamento das operações futuras. As novas necessidades de informações e outras não respondidas são a base para a actualização contínua do plano de pesquisa.

- c. Gestão da Pesquisa**

A gestão da pesquisa da informação tem quatro fases:

- **Avaliação de Necessidades e Recursos.** A avaliação de pedidos de pesquisa, PIR e dos meios que melhor podem responder às necessidades.
- **Preparação do Plano de Pesquisa.** Inclui:
 - Selecção de órgãos e meios.
 - Atribuição de ordens e pedidos de pesquisa aos órgãos.
- **Pesquisa da Informação.** Transmitir, à célula de informações, de forma atempada e precisa, as notícias para serem processadas e transformadas em informações.
- **Monitorizar e Reatribuir Tarefas.** As origens e órgãos relatam notícias, a qualidade dos relatórios é monitorizada, o plano de pesquisa actualizado e são atribuídas novas ordens de pesquisa aos órgãos.

0722. Pesquisa

- a. Generalidades**

A pesquisa é a segunda fase do Ciclo da Produção da Informação. Durante esta fase as origens de notícias e órgãos obtêm e distribuem notícias à célula de informações.

- b. Obtenção de Notícias**

Origens e órgãos obtêm notícias.

c. Distribuição das Notícias

A notícia originária de origens técnicas será por vezes pré-processada (alteração de formato), a fim de poder ser utilizada por pessoal não técnico. Contudo, devemos ter em conta que as notícias e informações são mais ou menos falíveis. A distribuição atempada é, por conseguinte, a essência.

(1) Pré-processamento das Notícias

Algumas origens, como a Guerra Electrónica, ou exploração de imagens e especialistas de Informações Técnicas, transformam aspectos específicos em notícias compreensíveis pela célula de informações.

(2) Deterioração das Informações e Notícias

O sistema de informações de combate serve para cumprir missões em situações de elevado ritmo operacional. Para tal:

- (a) As notícias de combate devem ser distribuídas o mais rapidamente possível à célula e unidades de informações para processamento e disseminação, antes que percam a sua importância como indicadores das capacidades e intenções do inimigo.
- (b) As informações devem ser rapidamente disseminadas antes de se tornarem inúteis como ferramenta de planeamento para o comandante, EM e unidades. Os comandantes necessitam de informações e não de notícias, para cumprir a missão com sucesso. Uma grande parte das indicações do comandante para o seu sistema de informações é o estabelecimento de fitas do tempo para reportar as informações.

A necessidade de produzir informações em tempo real de uma grande variedade de fontes requer a presença de especialistas das informações, com Normas de Execução Permanente (NEP) para manuseamento e processamento de informação e Sistemas de Informação e Comunicações (SIC) (CIS – *Communication and Information Systems*), que podem estabelecer a ligação às células de informações aos vários escalões de comando. A fim de obter informação em tempo real a partir de Aeronave Não-Tripulada (UAV – *Unmanned Aerial Vehicle*), é necessário integrar equipas de especialistas com equipamento SIC para processamento e exploração. De modo similar, outras origens como a guerra electrónica, artilharia e as unidades de reconhecimento devem possuir sistemas de comunicação robustos e interoperáveis com a célula de informações.

0723. Base de Dados das Informações

A base de dados das informações é o centro do sistema de informações de combate. A base de dados contém as informações básicas, notícias de combate e relatórios das informações fornecido pelas origens e produtos das informações disseminados pelos utilizadores. As bases de dados estão interligadas para proceder à troca automática das notícias e informações, de acordo com os níveis de segurança estabelecidos.

0724. Processamento

As notícias são convertidas em informações através dos seguintes passos:

- a. Registo.** Consiste no agrupamento sistemático de todas as notícias, criando um registo de acontecimentos, de forma a facilitar a sua ulterior transformação em informações e a elaboração de documentos de informações.
- b. Avaliação.** Consiste na apreciação de um item de informação relativamente ao grau de confiança da origem ou órgão de pesquisa e ao grau de verosimilhança da notícia.
- c. Análise.** Consiste em determinar e isolar os elementos significativos da notícia para subsequente interpretação.
- d. Integração.** Consiste na combinação dos elementos individualizados, obtidos por análise, com outras notícias ou informações já conhecidas, a fim de se formularem uma ou mais hipóteses lógicas.
- e. Interpretação.** Consiste na determinação do significado de uma notícia relativamente a outras notícias ou informações já existentes.

0725. Registo

É o processo de recepção, arquivo e registo de todos os relatórios que chegam à célula de informações. Envolve os registos de rotina de toda a informação recebida e a manutenção eficaz de bases de dados, por processos manuais ou electrónicos.

0726. Ferramentas de Registo

- a. Carta de Situação** – As notícias são registadas sobre as cartas, onde o nível de detalhe corresponde ao escalão da unidade. Por regra devem utilizar-se as escalas com o grau de detalhe suficiente para dois escalões abaixo.
- b. Ordem de Batalha** – Quando a identificação, potencial, estrutura de comando e dispositivo do inimigo são conhecidos, deve ser elaborada uma Ordem de Batalha (ORBAT – *Order of Battle*) a todos os escalões de comando com células de informações.
- c. Pasta de trabalho** – Os oficiais de informações mantêm uma pasta que contém os dados significativos para as informações. O conteúdo varia de acordo com o escalão do comando e área de emprego.
- d. Avaliação** – O objectivo da avaliação é determinar e indicar o grau de confiança atribuído a determinados itens da notícia recebida.

0727. Disseminação

A disseminação das informações ao nível tático segue os procedimentos detalhados no Capítulo 3.

0728. ISTAR ao Nível Tático

O ISTAR é descrito com detalhe no Capítulo 4.

0729. Planeamento ISTAR

A finalidade do planeamento ISTAR ao nível tático é obter a informação acerca de um inimigo que permita ao comandante a informação necessária ao sucesso do combate. O plano de pesquisa coordena os esforços de todas as origens. O plano de pesquisa pode incluir um transparente ISTAR. O processo de planeamento ISTAR inclui:

- Determinação das necessidades;
- Atribuição de prioridades;
- Desenvolvimento do plano;
- Pesquisa;
- Processamento;

- Reatribuição de missões aos órgãos de pesquisa.

O oficial de informações tem que compreender a missão e a intenção do comandante. Durante a análise da missão, o comandante estabelece os PIR, que são questões chave acerca do inimigo ou espaço de batalha que devem ser respondidas para o sucesso da operação. Os PIR devem questionar Quem? O quê? Quando? Onde? E Como?

Os oficiais de informações, através do conhecimento da doutrina do inimigo, identificam os indicadores nos quais os meios ISTAR são focalizados. Estes indicadores garantem respostas aos PIR, a outras necessidades de informações e de informação. Uma vez obtidas estas respostas, o oficial de informações dispõe de informações que irão auxiliar o comandante a entender o espaço de batalha.

O plano de pesquisa é desenvolvido para responder aos PIR e às necessidades de informação, sendo articulados os meios que permitem responder aos pedidos e ordens de pesquisa, de acordo com as suas capacidades.

Além dos meios orgânicos ou atribuídos, o oficial de informações deve estar familiarizado também com o plano de pesquisa do escalão superior que pode tornar redundantes alguns elementos do seu plano ou constituir um esforço adicional de pesquisa.

Página intencionalmente em branco

2^a PARTE

CONTRA-INFORMAÇÃO E SEGURANÇA

CAPÍTULO 8 INTRODUÇÃO

SECÇÃO I – CONCEITOS

0801. Conceitos

A condução efectiva, quer da Contra-Informação (CI – *Counter-Intelligence*) quer da Segurança, são essenciais para o sucesso operacional. Esta Parte fornece orientação doutrinária a todos aqueles cujo papel é conduzir CI e Segurança das Operações (OPSEC – *Operations Security*) e servirá de base à instrução de CI e Segurança. Serve, também, para permitir àqueles não directamente envolvidos na CI e na Segurança, a compreensão destas duas áreas, para que desempenhem um melhor papel na derrota da ameaça à segurança das forças amigas.

- a. A CI e a Segurança são duas áreas distintas mas interdependentes. Enquanto a primeira é activa e inclui a obtenção de informações de segurança e a neutralização da ameaça através da identificação das capacidades de Informações, Vigilância, Aquisição de Objectivos e Reconhecimento (ISTAR – *Intelligence, Surveillance, Target Acquisition and Reconnaissance*) do inimigo; a segunda é, simultaneamente, activa e defensiva e inclui todas as medidas de segurança e de protecção com vista a obter e manter a segurança.
- b. A CI é definida como o conjunto de actividades relacionadas com a identificação e neutralização da ameaça à segurança, constituída por serviços de informações e organizações hostis ou por indivíduos relacionados com espionagem, sabotagem, subversão ou terrorismo. Enquanto o comandante necessita das melhores informações possíveis sobre as capacidades e intenções do inimigo tentará, também, negar ao inimigo a oportunidade de obter notícias e informações sobre as capacidades, dispositivos e intenções das forças amigas, bem como das suas acções prováveis e vulnerabilidades. A CI preenche esta necessidade através da identificação e neutralização da ameaça constituída por elementos do ISTAR inimigo. Nega, igualmente, a informação ao inimigo e apoia a preservação e protecção das forças aliadas. O processo de CI identificará as vulnerabilidades das

PDE 2-00 Informações, Contra-Inteligência e Segurança

forças amigas à obtenção de notícias e informações por parte do inimigo e, assim, poderá apoiar a OPSEC, a Contra-Vigilância e o Plano de Decepção. A análise da CI classifica as operações do inimigo na Área de Operações (AOO – *Area of Operations*) das forças amigas, bem como as actividades de organizações subversivas na mesma área. A CI apoia as Informações e a Protecção da Força (FP – *Force Protection*).

- c. A Segurança é definida como a condição obtida quando a informação, o material, o pessoal, as actividades e as instalações estão protegidos contra a espionagem, a sabotagem, a subversão e o terrorismo, assim como contra perdas ou divulgações não autorizadas. A Segurança garante ao comandante, liberdade para planear e conduzir operações, reduzindo as vulnerabilidades às ameaças e actividades hostis. De igual modo, garantindo a segurança, o comandante ficará em melhores condições de conduzir as operações usando a surpresa. A Segurança contribui, de uma forma geral, para a FP, garantindo a manutenção do seu potencial de combate.

SECÇÃO II – A AMEAÇA À SEGURANÇA

0802. Actividades de Segurança

a. A ameaça à segurança compreende:

(1) Ameaça Directa

A ameaça directa mais óbvia é a assumida pelo inimigo. Durante a operação, o inimigo utilizará os seus meios de informações para:

(a) Obter notícias

Através da utilização de meios ISTAR com o objectivo de identificar a ordem de batalha, o dispositivo, as capacidades e intenções das forças amigas.

(b) Espionagem

Com o objectivo de descobrir, a longo prazo, as intenções, recursos e capacidades das forças amigas.

(c) Sabotagem

Destruição de pontos importantes ou materiais, nas operações conduzidas por Forças Especiais ou grupos de apoio local.

(d) Operações de Informação (INFO OPS – *Information Operations*)

Operações com a finalidade de destruir ou degradar a eficácia de combate das forças amigas.

(2) Ameaça Indirecta

Em todo o espectro do conflito, os potenciais inimigos tentarão melhorar a sua prontidão operacional e a sua capacidade económica para apoiar operações através de:

(a) Obtenção de Notícias

Pode ser realizada através de:

1 Recolha Aberta

A obtenção de notícias encontra-se disponível a partir de várias origens abertas. As notícias individuais podem ter pouco valor, mas quando relacionadas podem proporcionar informações precisas, ainda que de baixo nível.

2 Recolha Coberta

A informação sensível será cuidadosamente protegida. O inimigo deverá, portanto, efectuar acções deliberadas no sentido de obter notícias que lhe fornecerão informação válida a longo prazo.

(b) Subversão

Pode ser levada a cabo das seguintes formas:

1 Difundindo, abertamente, informação adulterada.2 Manipulando, secretamente, organizações potencialmente desleais.3 Infiltrando elementos nas organizações locais.4 Recrutando indivíduos desleais como agentes.

(c) Sabotagem

Destruir ou negar o acesso a material vital.

(d) Terrorismo

Embora nem sempre seja uma ameaça directa à força, o terrorismo afectará negativamente o ambiente no qual as operações são conduzidas. Assim, o terrorismo e as actividades a ele associadas, devem ser combatidas em conjunto com as entidades de segurança da Nação Hospedeira (HN – *Host Nation*).

PDE 2-00 Informações, Contra-Informação e Segurança

(e) Crime Organizado

Quando em grande escala, pode criar instabilidade económica no território onde a AOO se encontra inscrita.

(3) Operações de Informação

As INFO OPS por se incluírem em todas as actividades anteriores não serão tratadas de forma individualizada.

b. Origens da Ameaça

A ameaça tem origem, principalmente, em:

- (1) Serviços de Informações Hostis (HIS – *Hostile Intelligence Services*).
- (2) Organizações, grupos ou indivíduos subversivos.
- (3) Organizações, grupos ou indivíduos terroristas.
- (4) Unidades Especializadas do inimigo, tais como Forças Especiais.
- (5) Vigilância e reconhecimento aéreo, marítimo e terrestre, através de imagens e dispositivos de recolha de informações, incluindo satélites.
- (6) Organizações e grupos criminosos.
- (7) Indivíduos sem intenções claramente definidas.

- c.** Todas as actividades devem ser avaliadas em relação à situação actual das informações, na medida em que podem dar indicação das capacidades e intenções hostis.

SECÇÃO III – TIPOS DE AMEAÇA

0803. Espionagem

- a.** A espionagem pode ser descrita como um método utilizado pelos serviços de informações hostis, para obter informação que compromete a segurança nacional. Uma certa quantidade de informação válida está disponível, particularmente numa sociedade aberta e democrática. Pode ser obtida a partir de bibliotecas públicas e através da simples observação, entre outros meios abertos. A simples observação e a aquisição de informação através de origens abertas constitui, portanto, uma ameaça significativa à segurança, desenvolvida quer por organizações, quer por

indivíduos. Um serviço de informações hostil vocacionará, portanto, as suas actividades de espionagem para a obtenção de informação classificada que, por esse motivo, não é de fácil acesso. Deve ter-se em consideração que, mesmo notícias triviais podem ter um significado especial, quando tratadas e assimiladas por especialistas de informações. Para além disso, algumas das notícias obtidas por origens abertas necessitarão de ser confirmadas por outras origens.

- b.** Os HIS estão constantemente em busca de indivíduos com acesso, ou futuro acesso, a informação classificada ou outro material, que possam ser recrutados como agentes. Estes podem ser entre outros operadores de sistemas ou programadores entre outros. Existem várias razões que levam estes indivíduos a tornarem-se agentes, salientando-se as seguintes:

 - (1) Razões monetárias, outras compensações ou promessas de vários tipos.
 - (2) Vingança relativamente a situações reais ou imaginárias. Na sequência de uma acção comprometedora na qual um determinado indivíduo se viu envolvido e portanto sujeito a chantagem, por exemplo, casos amorosos, aberrações sexuais, actividades ilegais ou operações no mercado negro.
 - (3) Razões ideológicas.
- c.** Os avanços tecnológicos trouxeram ao agente dos nossos dias várias ajudas sofisticadas, tais como: dispositivos de escuta fácil e rapidamente instaláveis; microfotografia; copiadores de documentos simples e fáceis de esconder; câmaras de longo alcance; transmissores *Morse* de elevada velocidade. No entanto, como a espionagem é uma actividade dispendiosa e arriscada, uma operação só será montada se a informação não for passível de ser obtida de outro modo. Para além disso, devido aos custos e aos riscos, a espionagem tem tendência a ser selectiva, apesar de obviamente o inimigo poder aproveitar-se de qualquer negligência, acção ineficaz, falta de vigilância ou falhas na segurança.
- d.** Os principais objectivos da espionagem podem ser:

 - (1) As capacidades defensivas e ofensivas nacionais e aliadas.
 - (2) O desenvolvimento de armas e equipamento.
 - (3) As intenções nacionais.
 - (4) As bases de dados.

0804. Sabotagem

- a. Uma operação de sabotagem bem sucedida não tem, necessariamente, custos muito elevados na medida em que, utilizando uma pequena quantidade de explosivos ou material incendiário, um pequeno número de indivíduos ou mesmo um indivíduo apenas, pode criar toda uma perturbação muito para além do esforço necessário para a causar. A sabotagem ocorrerá principalmente em tempo de crise e guerra. Actos dispersos mas coordenados de sabotagem podem ser esperados imediatamente antes do início das hostilidades, numa altura em que o seu efeito será ampliado. No entanto, deverá ter-se em conta que no entanto, que uma acção de sabotagem poderá ser planeada e preparada antecipadamente em tempo de paz. O objectivo das acções de sabotagem não é necessariamente a destruição, mas a negação limitada da utilização das instalações atacadas.
- b. No entanto, os riscos associados a uma operação de sabotagem compelem o(s) sabotador(es) e aqueles que controlam e coordenam as actividades de sabotagem a ser extremamente selectivos. Devem seleccionar apenas os objectivos vitais, difíceis de recuperar ou para os quais não existe mesmo recuperação possível, e cuja destruição cause a máxima perturbação possível.
- c. A sabotagem deve ser dirigida particularmente a sistemas e tecnologias de informação, não apenas pelo ataque físico mas também por subversão, com vista a corromper o *software* e provocar a degradação no sistema, numa altura crítica.

0805. Subversão

- a. A subversão é definida como uma acção destinada para enfraquecer a força militar, económica ou política de uma nação pelo enfraquecimento do moral, da lealdade e da confiança dos seus cidadãos. Um ataque à lealdade de um indivíduo ou grupo é uma acção perturbadora, difícil de detectar ou contrariar.
- b. Uma organização subversiva adopta métodos ilegais ou inconstitucionais de forma a provocar uma mudança no governo favorável à organização. Os próprios indivíduos podem também ser subvertidos para que a sua lealdade pessoal se altere e, subsequentemente, se tornem utilizáveis por órgãos hostis ou organizações subversivas. Existem várias técnicas de subversão e métodos modernos de comunicação – jornais, rádio, televisão e *internet* – com grande

audiência ao alcance de indivíduos, grupos ou organizações subversivas. Os seus métodos de subversão podem incluir:

- (1) A propaganda e a agitação, manifestações, tumultos e distribuição de panfletos.
- (2) A utilização de “histórias de cobertura”¹⁸ para esconder as actividades reais.
- (3) O recrutamento de “apoiantes” que operam, tanto consciente como inconscientemente, em seu benefício.
- (4) A criação de um clima de desconfiança e desilusão que leve ao descrédito de governos e indivíduos.
- (5) A divulgação de falsos rumores ou verdades distorcidas com o objectivo de destruir a confiança nos líderes ou aliados.

- c. Em tempo de paz, a subversão é a ameaça mais comum à segurança e que ocorre de uma forma contínua. Em tempo de crise, é provável que a subversão aumente. A subversão poderá não ser apenas conduzida como atrás se descreve. Em algumas nações democráticas, marchas e demonstrações devidamente sancionadas, publicações reconhecidas oficialmente e outros produtos dos *media* poderão ter, também, natureza subversiva.

0806. Terrorismo

- a. O terrorismo pode ser definido como a utilização ilegal, de forma efectiva ou potencial, da força ou violência contra pessoas ou bens, tentando coagir ou intimidar governos ou sociedades, para alcançar objectivos políticos, religiosos, étnicos ou ideológicos. O terrorismo, apesar de ser efectivamente uma extensão da subversão, disseminou-se de tal forma que deve ser encarado como uma ameaça, por si só.
- b. A condução do terrorismo pode incluir o uso de:
- Perseguição e ameaças;
 - Propaganda;
 - Furto de dinheiro, armas ou outro equipamento;
 - Ataques armados, ataques bombistas e julgamentos;

¹⁸ São situações ou organizações criadas para encobrir actividades.

PDE 2-00 Informações, Contra-Inteligência e Segurança

- Assassinatos e raptos;
- Meios/dispositivos nucleares, biológicos, químicos e radiológicos.

0807. Crime Organizado

- a. O crime organizado pode ser descrito como as acções de organizações de natureza criminosa, estruturadas em rede, com um ou mais líderes e várias unidades subordinadas espalhadas num vasto território. O objectivo do crime organizado é obter, ilegalmente, alguma forma de poder através de influências ou dinheiro, desrespeitando as leis democráticas em vigor no país no qual o crime organizado está a operar.
- b. Podem ser desenvolvidas actividades criminosas semelhantes às descritas no parágrafo anterior e, para além delas, contrabando, operações ilegais de tráfico de drogas e de pessoas, numa escala que pode pôr em perigo a segurança nacional e militar de um país.

SECÇÃO IV – NEUTRALIZAÇÃO DA AMEAÇA

0808. Responsabilidade pela Neutralização da Ameaça

- a. A ameaça à segurança pode ser neutralizada através da CI e de medidas de protecção e segurança. As organizações de CI, militar ou civil, das nações pertencentes à Organização do Tratado do Atlântico Norte (OTAN) são responsáveis pela neutralização da ameaça à segurança constituída por HIS, organizações subversivas e grupos terroristas ou criminosos. Os comandantes a todos os níveis são responsáveis pela segurança e pelo esforço de CI.
- b. A CI e os elementos responsáveis pela segurança são estabelecidos a todos os níveis de comando:
 - (1) Nível Estratégico

Ao nível estratégico o pessoal da CI e da Segurança é responsável pela direcção geral da CI e da Segurança no Teatro de Operações (TO). Tal incluirá o desenvolvimento da CI e da Arquitectura de Segurança como parte do Plano

de Gestão de Informações e da alocação e organização dos recursos de CI e segurança.

(2) Nível Operacional

Ao nível do Quartel-General da Força Tarefa Conjunta Combinada (CJTFFHQ – *Combined Joint Task Force Headquarters*) o Estado-Maior (EM) terá elementos da CI Conjunta e de segurança para aconselhar o comandante e coordenar estas actividades. Dependendo da natureza da operação, esta pode ser apoiada por analistas especializados em CI que orientarão a produção de informações de segurança de todas as origens e a manutenção dos registos de segurança e bases de dados. A célula de informações no CJTFFHQ é responsável pela produção do estudo da situação da CI.

(3) Nível Tático

Os elementos de EM responsáveis pela segurança aconselham o comandante em assuntos de CI e de Segurança. Estes elementos trabalham em estreita colaboração com os elementos do EM ISTAR, os quais são responsáveis pela produção do estudo da situação de CI. A unidade ou subunidade de Informações Militares poderá, também, fornecer informação sobre a ameaça, apoiar a CI e aconselhar, em assuntos de segurança, a instrução e os Oficiais de Segurança das unidades.

c. As principais responsabilidades dos elementos de EM de CI e de segurança, em todos os níveis de comando, são:

- (1) Aconselhar o comandante em todos os assuntos relativos à segurança.
- (2) A gestão da CI e da segurança a cada nível de comando.
- (3) O processamento da informação de segurança e a disseminação de avaliações actualizadas da ameaça.
- (4) A contribuição para o processo de OPSEC, incluindo o planeamento, coordenação e a aplicação de medidas de protecção de segurança em toda a força.
- (5) A gestão, quando apropriado, de unidades de segurança.
- (6) O estabelecimento e manutenção da ligação com as autoridades policiais.

SECÇÃO V – PRINCÍPIOS ORIENTADORES DA CI E DAS OPERAÇÕES DE SEGURANÇA

0809. Princípios

As operações de CI e de segurança devem ser conduzidas de acordo com os seguintes princípios:

- Os comandantes, a todos os níveis, são responsáveis pela segurança e devem dirigir o esforço de CI.
- As operações de CI e de segurança devem ser geridas pela célula das informações, em conjugação com a das operações e outras, devendo ser integradas no esforço geral das informações.
- Em cada nível de comando, para cada política de segurança deve existir um ponto de convergência.
- Em cada nível de comando, devem ser estabelecidas equipas de CI e de segurança para gerir as actividades relacionadas com segurança e para apoiar os comandantes.
- O pessoal da CI e da segurança deve produzir informação relativa ao nível de ameaça, sob a forma de alertas, avaliações e anúncios, atribuindo-lhes o mais baixo nível de classificação possível e garantindo a sua disseminação o mais rapidamente possível.
- A actividade de pesquisa de informação de segurança deve ser coordenada em cada escalão de comando e integrada no esforço de pesquisa de informações.
- A responsabilidade pelo estabelecimento e manutenção das bases de dados da informação de segurança deve ser claramente definida e, sempre que possível, integrada no esforço das informações ao nível do TO.

CAPÍTULO 9 CONTRA-INFORMAÇÃO

SECÇÃO I – O PAPEL DA CONTRA-INFORMAÇÃO

0901. O Papel da Contra-Informação

- a. A Contra-Informação (CI – *Counter-Intelligence*) está relacionada com a identificação e neutralização da ameaça constituída pelo sistema de Informações, Vigilância, Aquisição de Objectivos e Reconhecimento (ISTAR – *Intelligence, Surveillance, Target Acquisition and Reconnaissance*) inimigo e por organizações subversivas. Contribui para a negação da informação ao inimigo e para a preservação e protecção da força amiga.
- b. De forma a permitir ao comandante planear e executar com sucesso operações militares, deverá negar ao inimigo notícias e informações relativas às capacidades, dispositivos, intenções e acções prováveis da força amiga. A CI fornecerá ao Comandante as informações que permitam esclarecer quais as notícias e informações que apoiam o processo da tomada de decisão do inimigo e a selecção da sua modalidade de acção. Poderá, também, identificar a vulnerabilidade da força amiga às operações de recolha de informações do inimigo e, desta forma, informar a Segurança das Operações (OPSEC – *Operations Security*), a contra-vigilância e o planeamento de decepção incluindo a política de Segurança de Protecção.
- c. A CI identifica as operações do inimigo na Área de Operações (AOO – *Area of Operations*) e as actividades das organizações subversivas. Todas estas acções implicarão, provavelmente, a recolha e processamento da informação, bem como a execução de operações de informações. Algumas delas poderão ter o cariz de uma operação ofensiva convencional. A detecção e identificação destas operações e actividades salientam a importância das Informações de Segurança (SI – *Security Intelligence*).¹⁹

¹⁹ São definidas como informações sobre a identidade, potencialidades e intenções de organizações hostis ou indivíduos que estão ou podem vir a estar envolvidos em actividades de espionagem, sabotagem, subversão ou terrorismo.

SECÇÃO II – NORMAS DA CONTRA-INFORMAÇÃO

0902. Introdução

As nações pertencentes à Organização do Tratado do Atlântico Norte (OTAN) entendem que uma estreita ligação entre as organizações nacionais de CI, aos vários níveis, e os comandos militares OTAN adequados, conduzirá a um maior conhecimento e compreensão da situação e dos problemas com ela relacionados, em tempo de paz. Para além disso, tal ligação irá estabelecer o enquadramento para a passagem de uma situação de paz para uma situação de crise. Nos parágrafos seguintes são apresentadas as directivas a seguir as quais determinam os requisitos dos Comandos da OTAN para a CI e os pontos de contacto entre os Comandos da OTAN e as autoridades nacionais.

0903. A Contra-Informação em Operações Multinacionais

- a. Quando as forças se encontram destacadas em Operações de Resposta a Crises (CRO – *Crisis Response Operations*), a Autoridade responsável pela Segurança no Teatro supervisionará todos os aspectos de CI e será o principal conselheiro do Comandante em assuntos de CI.
- b. É responsabilidade nacional decidir a extensão e o nível de troca de CI. No entanto, as nações são responsáveis pelo fornecimento de CI de forma a permitir à OTAN e/ou aos comandantes das forças de coligação no teatro reagirem contra a ameaça em CRO para contrariar, com sucesso, a ameaça existente e em mudança constante é essencial uma troca de CI suficiente e atempada.
- c. Tomando como referência o exemplo da OTAN, os Comandantes dos Comandos Estratégicos (SC – *Strategic Commands*) e os seus conselheiros de CI só estarão em condições de cumprir as suas responsabilidades se puderem contar com uma estreita colaboração por parte das autoridades nacionais, uma vez que são estas que detêm o controlo dos seus organismos de CI (outras que não aquelas ligadas às forças OTAN). A colaboração em tempo de conflito só pode ser assegurada por ligações estabelecidas em tempo de paz. Num conflito deve ser evidente que as nações OTAN são responsáveis pelo preenchimento dos requisitos de CI gerais e específicos determinados pelos SC e pelos comandantes subordinados.

SECÇÃO III – PROCESSO DE CONTRA-INFORMAÇÃO

0904. Processo de Contra-Inteligência

De forma a assegurar que a CI é sempre conduzida da forma mais eficaz e comum a todas as nações da Aliança, foram desenvolvidas directivas para uma metodologia padrão. Trata-se do processo de CI. Este processo – tal como outros processos de informações – é baseado no Ciclo da Produção da Informação. A relação entre o Processo de CI e o Ciclo da Produção da Informação está representado na Figura 9-1.

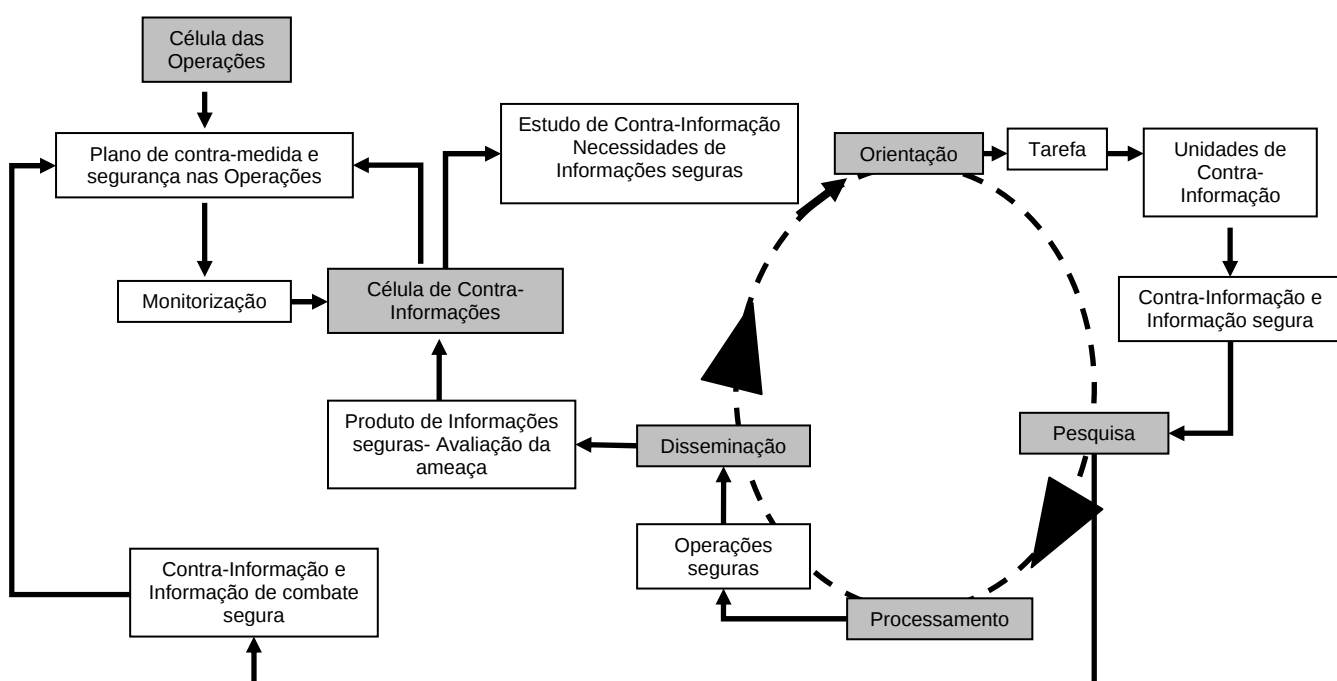


Figura 9-1 – Relação entre o Processo de CI e o Ciclo da Produção da Informação

0905. Estudo de Contra-Inteligência

- a. Esta é a fase em que o Processo de CI, quando em paralelo com a produção do Estudo da Situação de Informações Conjunto pela Célula de Informações, auxilia o processo de planeamento e a tomada da decisão pelo comandante. O estudo de CI centraliza-se nas capacidades ISTAR do inimigo, na ameaça constituída por organizações terroristas e subversivas e na vulnerabilidade da força aliada ao ISTAR inimigo e a outras ameaças que serão produzidas pelo ISTAR. O estudo de CI fornece a orientação para o restante Processo de CI.

PDE 2-00 Informações, Contra-Inteligência e Segurança

- b.** O estudo de CI apoiará e complementarará o Estudo da Situação de Informações Conjunto:
 - (1) Fornecendo um estudo da vulnerabilidade da força aliada às informações do inimigo e operações de recolha de informações, tendo por base os meios de contra-vigilância, OPSEC e planeamento de decepção.
 - (2) Transmitindo informação, apoiando o processo da tomada de decisão, o que influenciará a selecção da modalidade de acção mais provável a desenvolver pelo inimigo.
 - (3) Auxiliando na identificação de actividades prováveis do inimigo na retaguarda da força aliada e, desta forma, contribuindo para a Protecção da Força.
- c.** O Estudo de CI contribui para a formulação das Necessidades de Informações de Segurança (SIR – *Security Intelligence Requirements*).

0906. Planeamento de Contra-Inteligência

- a.** A exploração atempada de objectivos de CI requer a formulação de um planeamento coordenado de CI. No Plano de CI, é dada relevância aos objectivos de forma a indicar o grau de ameaça que representam e consequentemente o grau de urgência com que deverão ser neutralizados ou explorados e ligados a contra-medidas adequadas aos resultados pretendidos retirados do Plano de CI.
- b.** A CI, a participação e o apoio no domínio da segurança devem ter implicações na fase inicial de planeamento das operações. Deve ser dada particular atenção à identificação das vulnerabilidades da força amiga que podem ser exploradas pelos dispositivos ISTAR do inimigo e à determinação de contra-medidas adequadas.
- c.** A determinação das necessidades para orientar a pesquisa de informações de segurança deverá seguir os mesmos procedimentos que os utilizados para outras formas de informações. Com base nas conclusões do estudo de CI, deverá ser preparada uma folha de trabalho, que constituirá a base do planeamento, preparação de directivas e pedidos de informações mais completas.

0907. Pesquisa de Contra-Inteligência

A pesquisa de CI é conduzida recorrendo à Informação Humana (HUMINT – *Human Intelligence*) e outros meios de pesquisa ISTAR, com recurso a meios orgânicos e a produção de Pedidos de Pesquisa (RFI – *Request For Information*) para meios não-orgânicos. Na prática, as Necessidades de Informação (IR – *Information Requirements*) são efectuadas de acordo com o Plano de Pesquisa. Inevitavelmente, verificar-se-ão pedidos simultâneos para a utilização dos mesmos meios de pesquisa. O comandante deverá estar preparado para estabelecer e alterar prioridades para utilização destes meios à medida que a situação operacional evolui.

0908. Avaliação da Ameaça

- a. O desenvolvimento da avaliação da ameaça é o primeiro passo a ser tomado para neutralizar a ameaça e é de extrema importância, pois todas as outras medidas de segurança derivam dele. Assim sendo, cada nação, cada organização de CI e cada nível de comando deve efectuar uma avaliação cuidadosa da ameaça que deve ser constantemente revista e corrigida de acordo com os novos conhecimentos ou alterações da situação operacional. O processo de avaliação da ameaça equivale à fase de Processamento do Ciclo da Produção da Informação e a avaliação da ameaça, por si só, é difundida como produto de informações de segurança.
- b. As avaliações da ameaça deverão, sempre que possível, ser baseadas em informações de segurança actuais e atempadas, definidas pelo estudo de CI e por estudos de todas as organizações e entidades relevantes. Mais informações podem ser obtidas, acedendo aos serviços de informações hostis, bem como a organizações subversivas, criminais e terroristas. As informações recolhidas devem ser processadas e disseminadas como produto de CI, de acordo com o ciclo da produção da informação. Este produto de CI será um dos maiores contributos para a avaliação da ameaça. A avaliação da ameaça incluirá as avaliações:
 - (1) De elementos da força adversária que constituem ameaça à segurança das operações e da força amiga.
 - (2) Das capacidades e intenções do inimigo para produzir ataques de informações, através do seu sistema ISTAR e ainda para desenvolver acções letais.
 - (3) Dos métodos que serão, provavelmente, empregues pelo inimigo na conduta destas operações.
 - (4) Dos objectivos que serão, provavelmente, atacados.

0909. Contra-Medidas de Contra-Informação**a. Implicações para a Segurança da Força**

Os serviços de informações podem deduzir, da avaliação da ameaça, os efeitos que as várias ameaças identificadas poderão ter na escolha da modalidade de acção por parte da força amiga. Estas dividem-se em:

(1) Problemas a Neutralizar

Relacionados principalmente com a conduta de medidas de segurança e OPSEC eficazes.

(2) Oportunidades a Explorar

Ir ao encontro de necessidades de informação e da conduta de operações de informação (INFO OPS – *Information Operations*) através de operações psicológicas (PSYOPS – *Psychological Operations*) e da decepção.

b. Contra-Medidas

As Contra-Medidas abrangem tarefas em todo o espectro de CI e Segurança e têm quatro objectivos principais:

(1) Dissuadir

Medidas evidentes e sólidas constituirão um elemento de dissuasão eficaz contra um potencial atacante. No entanto, mesmo o conhecimento de que medidas menos evidentes para inviabilizar o acesso e detectar intrusão tenham sido introduzidas, constituirá um elemento de dissuasão a operações físicas ou de informações por parte do inimigo.

(2) Negar

Actividades desenvolvidas para evitar que o inimigo tenha acesso a informação sensível e protegida, prevenindo a subversão do pessoal e a passagem das barreiras de segurança física da força aliada.

(3) Detectar

A exposição e neutralização dos esforços inimigos de operações de recolha de informações e actividades ISTAR.

(4) Decepção

Actividade realizada para conduzir o inimigo a uma avaliação errada sobre as capacidades e intenções da força amiga.

c. Objectivos da Contra-Informação

Quando a avaliação da ameaça for efectuada e as implicações para a segurança da força forem identificadas, os objectivos da CI podem ser identificados. Os objectivos da CI são instalações, organizações e personalidades ou interesses de informações ou contra-informações que devam ser obtidas, destruídas, exploradas ou protegidas.

SECÇÃO IV – AS NECESSIDADES DE CONTRA-INFORMAÇÃO**0910. Necessidades de Contra-Informação**

Os comandantes com responsabilidades de CI necessitam de informação e apoio CI para cumprirem as suas missões. Estas necessidades podem ser classificadas do seguinte modo:

a. Necessidades Primárias de CI

Informação sobre serviços de informações não-OTAN e organizações subversivas, grupos terroristas e criminosos contra a OTAN e/ou nações membros da OTAN.

b. Necessidades Actuais de CI

Informação oportuna que pode fornecer uma clarificação adicional e um conhecimento alargado sobre serviços de informações não-OTAN e organizações subversivas, grupos terroristas e criminosos e as suas actividades, tais como: espionagem, sabotagem, subversão, terrorismo e crime organizado.

c. Necessidades Urgentes de CI

Informação atempada sobre actividades requerendo contra-medidas imediatas por parte de autoridades OTAN e/ou nações membros da OTAN.

Página intencionalmente em branco

CAPÍTULO 10 SEGURANÇA NAS OPERAÇÕES

SECÇÃO I – AVALIAÇÃO DA AMEAÇA

1001. Generalidades

A avaliação da ameaça constitui uma medida importante a ser levada em consideração para a sua neutralização, pelo que deve ser efectuada da seguinte forma:

- Estudando as potencialidades, capacidades, métodos e intenções prováveis de actuação de todas as organizações, grupos, indivíduos e respectivos meios;
- Considerando a ameaça à vulnerabilidade de alvos críticos;
- Identificando possíveis objectivos com maior probabilidade de serem atacados.

SECÇÃO II – MEDIDAS DE PROTECÇÃO

1002. Definição

- a. As medidas de protecção são definidas como um sistema organizado de medidas defensivas estabelecidas e mantidas a todos os escalões de comando com o objectivo de alcançar e manter a segurança. Trata-se da protecção dos meios, incluindo pessoal, de acontecimentos não desejados ou de um acordo.
- b. Existem quatro categorias de medidas de protecção, nomeadamente:
 - (1) Segurança do Pessoal.
 - (2) Segurança Física.
 - (3) Segurança Organizacional.
 - (4) Segurança da Informação (INFOSEC – *Information Security*) e Processamento Automático de Dados (ADP – *Automatic Data Processing*).
- c. As medidas de segurança são estabelecidas com base na avaliação de ameaça atrás mencionada.

1003. Medidas de Segurança do Pessoal

Estas medidas compreendem:

- a. Selecção de pessoal para funções sensíveis.
- b. Autorização para o pessoal seleccionado ter acesso a informação classificada obedecendo ao princípio da “necessidade de conhecer”.
- c. Investigação acerca do carácter e dos antecedentes do pessoal a seleccionar para o desempenho de funções sensíveis, assim como do cônjuge ou companheiro, de acordo com o permitido pela legislação em vigor. O objectivo é evitar que indivíduos duvidosos tenham acesso a informação classificada. No entanto, esta investigação permite apenas estabelecer que, numa determinada data, um determinado indivíduo é ou não de confiança.
- d. Manutenção, dentro do contexto da supervisão geral, de uma vigilância constante sobre a integridade dos indivíduos com acesso a informação classificada.
- e. Eficácia no âmbito da gestão dos recursos humanos, supervisão e formação.

1004. Medidas de Segurança Física

- a. Estas medidas implicam:
 - (1) O emprego de guardas e de forças de reacção, bem como de medidas estruturais e de técnicas, tais como obstáculos físicos, colocados em profundidade, para frustrar eventuais tentativas de penetração nos sistemas de segurança.
 - (2) O estabelecimento de medidas para evitar eventuais intromissões através de dispositivos electrónicos, acústicos e ópticos (TSCM – *Technical Surveillance Counter-Measures*).
- b. No entanto, os melhores dispositivos de segurança pouco mais podem provocar que o retardamento de uma intromissão, uma vez que um intruso determinado e eficaz terá sempre sucesso. Todavia, uma vez que os pré-requisitos do sucesso da espionagem é de que os detentores de informações secretas não devam ser alertados para o facto de essas informações serem do conhecimento do inimigo, a

segurança física deve ser apoiada por outras medidas que, num prazo tão curto quanto possível, revelem as actividades de um intruso. A vantagem da segurança física é a de tornar a penetração nos sistemas de segurança mais difícil e, conseqüentemente, garantir tempo para que outras medidas de segurança sejam adoptadas.

1005. Medidas de Segurança Organizacional

As medidas de segurança organizacional dependem em grande parte da aplicação de certos procedimentos que fazem parte das normas, leis, ordens, instruções ou Normas de Execução Permanente (NEP) (SOP – *Standing Operating Procedures*) da Organização do Tratado do Atlântico Norte (OTAN), nacionais ou das próprias unidades. Destes procedimentos fazem parte:

- a. Designação de zonas consideradas de alta ou baixa segurança.
- b. Agrupamento de zonas de alta ou de baixa segurança.
- c. Fornecimento de guardas e respectivo apoio.
- d. Sistemas de segurança para passagem.
- e. Controlo de acesso a áreas restritas ou proibidas.
- f. Desenvolvimento de planos de contingência ao Plano de Segurança, incluindo controlo de tumultos e de pontos importantes, assim como a criação de um adequado sistema de estados de alerta.
- g. A inclusão nas ordens em vigor de todos os Planos de Segurança, incluindo inspecções regulares, vigilância e verificações para assegurar que as medidas de protecção estão a ser cumpridas e continuam actuais e eficazes. Quando eficazes, as medidas de segurança organizacional poderão evitar tentativas de intromissão e conduzir a uma investigação. As inspecções de segurança pretendem revelar vulnerabilidades no sistema de protecção. O objectivo da investigação de segurança é identificar e solucionar eventuais falhas.

PDE 2-00 Informações, Contra-Informação e Segurança

- h.** Classificação apropriada de documentos, material e equipamento.
- i.** Planeamento e fornecimento de equipamento para a destruição de material classificado, quer em situação normal quer em caso de emergência.
- j.** Treino de segurança na forma de:

 - (1) Briefings de segurança, os quais deverão ser dirigidos para o pessoal militar, fornecendo informação sobre os antecedentes ideológicos, os métodos e os objectivos das organizações subversivas/terroristas/criminosas e os serviços de informações hostis.
 - (2) Treino de segurança cobrindo a situação de segurança, a ameaça e as NEP de segurança.
 - (3) Exercícios de segurança que põem em acção planos de contingência em situações de emergência.
 - (4) Treino de segurança relacionado com o ADP, tanto para os operadores como para o restante pessoal que trabalha na área da segurança.
- k.** Implementação de censura (determinada pela legislação nacional/liberdade de informação).
- l.** Procedimentos de segurança dos aeródromos a fim de estabelecer áreas restritas para aeronaves militares (inclui todos os tipos de veículos aéreos de asa fixa ou móvel, dirigíveis e balões). Estes procedimentos fazem parte da rotina organizacional e das medidas de segurança física; no entanto, os procedimentos para as áreas restritas da OTAN e aeronaves militares dos países OTAN, quando utilizem aeródromos militares de outras nações OTAN, revestem-se de especial interesse e serão estabelecidos nas seguintes condições:

 - (1) Quando requisitado, através dos canais diplomáticos da OTAN, pela nação visitante/Comando OTAN.
 - (2) Como resultado de uma emergência aérea.
 - (3) Através de acordos bilaterais entre as nações OTAN, os quais incluam os pontos anteriores.

1006. Medidas de Segurança da Informação e Processamento Automático de Dados

De forma a evitar o acesso não autorizado à informação digital, deverão ser tomadas as seguintes medidas, a menos que as autoridades nacionais dêem instruções noutra sentido:

- a. Os sistemas ADP deverão ser operados, tal como o equipamento armazenado, apenas em áreas restritas com acesso limitado.
- b. O acesso ao sistema só deverá ser autorizado ao pessoal credenciado ao mais alto nível da classificação da informação ou dos dados no sistema.
- c. O acesso aos sistemas ADP através de dispositivos electrónicos (CD-ROM, Disquetes, etc.) deve ser limitado e controlado.
- d. O equipamento ADP aprovado pela TEMPEST²⁰ deverá ser utilizado sempre que as condições existentes não corresponderem a um determinado padrão, sobretudo quando os sistemas ADP estiverem colocados no terreno.
- e. A alteração frequente de senhas (*passwords*) deverá ser obrigatória.
- f. As redes militares não deverão estar ligadas a redes públicas como a *internet*, a menos que meios técnicos seguros possam evitar o acesso não autorizado.

SECÇÃO III – NEUTRALIZAÇÃO DA AMEAÇA**1007. Responsabilidade**

- a. As nações hospedeiras são primariamente responsáveis pela protecção externa das instalações OTAN localizadas no seu território. Deverão ser desenvolvidos planos nacionais e ligações estreitas entre os Estados-Maiors nacionais e os Comandos da OTAN.

²⁰ TEMPEST é o nome de código para o conjunto de normalizações que limitam radiações eléctricas ou electromagnéticas de equipamentos electrónicos, tais como microchips, monitores ou impressoras. É uma medida de CI com vista a prevenir a espionagem.

PDE 2-00 Informações, Contra-Inteligência e Segurança

b. A ameaça é encontrada da seguinte forma:

- Proporcionando a manutenção adequada da segurança na fase inicial do planeamento, particularmente na construção de instalações e serviços do governo. Tal procedimento poderá significar uma redução significativa dos custos a longo prazo;
- Concentrando, o que houver a proteger, numa área mais pequena possível;
- Estabelecendo medidas de protecção na profundidade;
- Reforçando os padrões mínimos comuns de segurança física;
- Emitindo ordens de segurança práticas e sensatas;
- Instruindo o pessoal em termos de segurança;
- Treinando o pessoal directamente responsável pela segurança, particularmente em contrariar a subversão e ataques ideológicos, fornecendo-lhe informação e conhecimentos adequados;
- Aplicando os princípios da “necessidade de conhecer” e da “necessidade de explorar os conhecimentos”;
- Conduzindo inspecções, supervisões e verificações de segurança com regularidade;
- Utilizando especialistas em segurança;
- Colaborando com os especialistas em Contra-Inteligência (CI – Counter-Intelligence) e Segurança, procurando aceitar as suas recomendações e opiniões.

SECÇÃO IV – PROTECÇÃO DA FORÇA

1008. Generalidades

- a.** Quando as tropas estiverem no terreno, especialmente durante as Operações de Resposta a Crises (CRO – *Crisis Response Operations*), para além da condução da própria operação, deve ser dada ênfase à protecção do pessoal, à propriedade, ao equipamento, aos recursos críticos da OTAN e das forças de coligação no Teatro e às nações hospedeiras. Todas as acções necessárias para o efeito estão incluídas no termo “Protecção da Força” (FP – *Force Protection*).

- b. A FP é um processo que visa a conservação do potencial de combate de uma força preservando a sua integridade e capacidade, contrariando as ameaças aos seus elementos por parte do inimigo, por perigos naturais e ambientais e ainda pelos fogos fratricidas.
- c. Na avaliação de risco da força um vasto leque de factores deve ser considerado. Num dos extremos encontram-se as operações ofensivas adversárias conduzidas pelas suas forças principais e, no outro, os assuntos ambientais. A FP integra tanto o nível da força como o nível das medidas de protecção colectivas, tais como: Defesa Aérea, Segurança Ambiental e Segurança das Operações (OPSEC – *Operations Security*), incluindo a Contra-Vigilância e a Decepção, com medidas de segurança física de âmbito local adequadas à força.

1009. Objectivos da Protecção da Força

Os objectivos da FP são:

- a. Reduzir os riscos constituídos pelo inimigo às operações, às informações, ao pessoal, ao material e às instalações, para permitir, sem interferências, a condução das operações e as actividades de rotina.
- b. Reduzir a incerteza criada pelo inimigo e incentivar um sentimento de bem-estar, de segurança e de confiança.
- c. Facilitar e incrementar as operações e outras actividades.

SECÇÃO V – COMPONENTES DA PROTECÇÃO DA FORÇA

1010. Introdução

- a. A FP é a estrutura total que integra os vários componentes individuais. Cada componente pode ser conduzida individualmente; porém, quando diferentes componentes são integradas dentro da estrutura da FP, o benefício é maior.

PDE 2-00 Informações, Contra-Inteligência e Segurança

- b. Esta secção contempla as três componentes activas da FP: a OPSEC, a Contra-Vigilância e a Decepção e explica como as Medidas de Protecção, a Segurança no Terreno e a CI, contribuem para a FP.

1011. Segurança das Operações

- a. A OPSEC é o processo que confere a uma operação militar ou exercício a segurança apropriada, usando meios activos ou passivos, para negar ao inimigo o conhecimento dos dispositivos, das capacidades e das intenções das forças amigas. A OPSEC é uma responsabilidade do comandante e uma função da área das Operações. O processo faz parte do planeamento operacional. A condução da OPSEC não retira a necessidade das tradicionais medidas de segurança serem executadas, a fim de assegurar continuamente a segurança táctica e a protecção.
- b. A OPSEC cobre um vasto leque de áreas militares. Em termos ofensivos, romper ou destruir a capacidade de Informações, de Vigilância, de Aquisição de Objectivos e de Reconhecimento (ISTAR – *Intelligence, Surveillance, Target Acquisition and Reconnaissance*) do inimigo. Em termos defensivos, negar informação ao inimigo. O seu principal objectivo é impedir que o inimigo desenvolva um entendimento das intenções e das vulnerabilidades das nossas forças. Por outras palavras, distorcer a avaliação da situação do inimigo. A OPSEC protege unicamente a informação crítica, não se envolvendo com a protecção física de pessoal.
- c. A condução da OPSEC consiste em examinar todos os aspectos de uma determinada operação, à luz do conhecimento do inimigo ou das capacidades ISTAR suspeitas, para identificar esses indicadores a partir dos quais o inimigo pode deduzir informação e informações sobre uma organização ou operação. Estes indicadores garantem uma protecção apropriada dos meios ISTAR do inimigo. A OPSEC não tem por objectivo proteger toda a informação ou esconder toda a actividade militar todavia deve ser executada uma avaliação do risco. Uma elevada actividade OPSEC implica um gasto excessivo de recursos, limitando a actividade operacional. Por sua vez, uma baixa actividade OPSEC permite uma maior liberdade de acção mas aumenta o risco.

- d. As medidas de OPSEC incorporam muitas medidas de protecção, nomeadamente Contra-Vigilância e a Decepção. A OPSEC contribui para a FP com vista a reduzir a ameaça a todos os elementos da força amiga.

1012. Contra-Vigilância

O inimigo instalará um vasto leque de sensores ISTAR para detectar e identificar as Forças Amigas no espaço de batalha. A contra-vigilância tem por objectivo evitar que o inimigo obtenha informação útil através destes meios que permita identificar e explorar as fraquezas nas Forças Amigas, as capacidades ou aspectos ligados à projecção da força. Um eficiente plano de contra-vigilância causará no inimigo a dúvida sobre a eficácia dos seus próprios sensores e levá-lo-á a perder a confiança na informação que eles adquirem. Nos níveis tático e operacional a camuflagem, a cobertura e a decepção têm a sua quota-parte no plano de contra-vigilância.

1013. Decepção

- a. O propósito da decepção é iludir o inimigo por manipulação, distorção ou falsificação de provas induzindo-o a adoptar uma modalidade de acção ou reacção que seja prejudicial aos seus interesses. Normalmente isto é alcançado pelo reforço de preconceitos ou percepções existentes, com o objectivo de convencer o inimigo a adoptar uma modalidade de acção. Os objectivos da decepção são obter:

(1) Surpresa

Um plano de decepção bem sucedido disfarçará ou ocultará as intenções amigas, as potencialidades, as vulnerabilidades e os dispositivos.

(2) Segurança

A decepção retrata uma falsa modalidade de acção amiga. Se o inimigo acredita que detectou a modalidade de acção amiga e os principais elementos da força amiga, isto permitirá segurança para as forças que estão realmente empenhadas tal como à verdadeira modalidade de acção.

(3) Liberdade de Acção

Ocupando as forças adversárias em encontrar uma suposta ameaça, o comandante garantirá uma maior liberdade de acção noutra parte do espaço de batalha.

(4) Economia de Esforço

Uma decepção bem sucedida limitará a perda de tempo e de recursos, assim como reduz as eventuais perdas humanas nas forças amigas.

PDE 2-00 Informações, Contra-Inteligência e Segurança

b. A decepção pode ser conduzida em todos os níveis das operações:

(1) Estratégico

A decepção ao nível estratégico é delineada para iludir o inimigo ao mais alto nível. Normalmente a decepção estratégica é prolongada no tempo e pode envolver um elevado número de organizações, incluindo órgãos nacionais desde o planeamento até à sua implementação. É planeada por uma equipa de especialistas – a mais restrita possível –, que trabalha directamente para o Comandante-Chefe ou para o ministro apropriado.

(2) Operacional

A decepção ao nível operacional cobre os planos de teatro com vista a corromper o inimigo sobre a condução das operações. Pode complementar um plano de decepção estratégico. Este nível de decepção é normalmente de curto prazo e apoia uma fase particular da operação.

(3) Tático

A decepção ao nível tático é de curto prazo e normalmente envolve elementos de decepção tais como a camuflagem, a cobertura e as fintas ao baixo escalão.

1014. Ligação da Contra-Vigilância, da Segurança das Operações e da Decepção

Estas três componentes são complementares. A contra-vigilância é essencial para a eficiência do plano OPSEC. A decepção necessita da eficiência da contra-vigilância e da integração do plano OPSEC para ocultar essas actividades que podem comprometer o falso quadro que está a ser retratado.

1015. Medidas de Protecção

a. Os objectivos das medidas de protecção são:

- Detectar qualquer tentativa, por parte de pessoal não autorizado, de aceder aos controlos.
- Evitar o acesso a informação por parte de serviços de informações hostis, organizações subversivas/criminais/terroristas e grupos ou indivíduos, causando perturbações ou subvertendo o pessoal militar ou civil.
- Fornecer padrões mínimos de segurança que possam ser aplicados em todas as unidades.
- Evitar a possibilidade de acesso não autorizado a informação digital e a destruição ou alteração da informação em redes ADP ou em computadores pessoais.
- Apoiar a investigação de especialistas nas falhas de segurança.

- b. Uma vez que nenhum controlo de segurança será eficaz isoladamente, as medidas de protecção devem consistir num determinado número de medidas de apoio interligadas, que permitam alcançar um grau de segurança aceitável.
- c. A aplicação das medidas de protecção é, principalmente, uma responsabilidade nacional. Grupos e forças destacadas noutros países aplicam medidas de protecção dentro da sua área de responsabilidade. Estas forças deverão coordenar as suas medidas de protecção com a nação hospedeira. A segurança das áreas de retaguarda continua a ser da responsabilidade da nação hospedeira. A troca de informações de segurança e a coordenação na aplicação de medidas de protecção são pré-requisitos para alcançar a segurança adequada.
- d. A CI e a INFOSEC são o ponto de partida para o planeamento e para a condução de medidas de protecção passivas e activas que deverão ser postas pelos comandantes, pelos seus elementos das informações e pelos meios de FP.

1016. Segurança no Terreno

- a. A segurança no terreno consiste no desenvolvimento e na implementação prática de contra-medidas de segurança a todos os escalões de comando, de forma a gerir o risco, proteger os meios militares preservando o potencial de combate. São necessárias actividades de CI de nível tático e de segurança de pessoal para identificar e neutralizar a ameaça. A segurança no terreno é principalmente conduzida ao nível do comando tático, por unidades de Informações Militares.
- b. As contra-medidas de segurança no terreno têm quatro objectivos principais: deter, dissuadir, detectar e enganar. São influenciadas pela análise da ameaça e pela natureza do deslocamento operacional.
- c. Ocorrerão inevitavelmente falhas na segurança. As investigações de segurança poderão revelar oportunidades a explorar. As operações de CI contra a recolha de informação por parte do inimigo ou actividades de organizações subversivas também contribuirão para a segurança.

PDE 2-00 Informações, Contra-Informação e Segurança

- d. Na segurança no terreno, a aplicação de actividades de CI de nível tático, envolvendo a aquisição de informação, a avaliação de ameaças locais e o desenvolvimento prático de medidas de segurança pessoal são a base para o esforço de CI sem o qual as medidas ao nível da Força serão infrutíferas.

1017. Passagem de Informação

- a. A informação relevante para a FP é recebida de um vasto conjunto de origens, especialmente de:
 - Origens humanas no Teatro, recolhidas por meios de Informação Humana (HUMINT – *Human Intelligence*) da OTAN ou nacionais (Informações, CI e Polícia Militar).
 - Informação de Comunicações (COMINT – *Communications Intelligence*).
 - Informações de fontes abertas (OSINT – *Open Source Intelligence*).
 - Serviços de Informações Nacionais e de órgãos de CI.
- b. Toda a informação disponível que dê entrada é integrada e processada (avaliada e analisada) pelos órgãos de Segurança responsáveis no Teatro, sendo o resultado transmitido aos Comandantes/Quartel-general (QG) respectivos, acompanhados de propostas claras de medidas de reacção/protecção adequadas.
- c. A integração de informação relacionada com a FP ocorre no Teatro, numa célula cobrindo todas as fontes no QG OTAN responsável. Esta célula deverá manter um contacto estreito com as Células Nacionais de Informações (NIC – *National Intelligence Cells*) que devem ser configuradas como células que cobrem todas as origens de informações.
- d. A informação vital para a FP, pelo seu impacto na avaliação da ameaça, não deve ser transmitida exclusivamente através dos canais habituais, mas levada imediatamente aos órgãos de segurança responsáveis no Teatro. As medidas para a FP, especialmente quando existe ameaça à vida dos militares, têm prioridade sobre todas as precauções de segurança habituais.

1018. Papel da Contra-Informação e Segurança

- a. Como referido anteriormente, a CI e a Segurança constituem uma parte importante do sistema de FP para as forças da OTAN e/ou forças de uma coligação, especialmente em Outras Operações Militares Que Não-Guerra (MOOTW – *Military Operations Other Than War*), como as Operações de Apoio à Paz (PSO – *Peace Support Operations*). A CI e a Segurança apoiam a FP. A FP não é uma subdivisão das Informações ou da CI e Segurança. As células de segurança no Teatro, quer nos QG nas forças da OTAN ou nos QG das forças de uma coligação, quer ainda num ambiente nacional com uma NIC, deverão constituir o ponto central de todas as actividades relacionadas com CI/ Segurança – FP.
- b. Normalmente é desejável que as capacidades dos diferentes componentes dos sistemas de Informações estejam ligadas entre si. Este sistema deverá ser constituído por elementos HUMINT, especialistas COMINT, operadores de CI, pessoal de segurança e analistas de informações.
- c. Esta capacidade deverá ser estabelecida de forma rápida e integrada na estrutura do QG, após o início da projecção das forças. Para efeitos de ligação e coordenação devem ser designados pontos de contacto. Num QG, será o CJ2X²¹ o elemento responsável pela coordenação e resolução de conflitos relativamente a todas as operações de HUMINT e CI e dispositivos na sua área de responsabilidade. Se estiver estabelecido o NIC no TO em apoio ao contingente nacional assim como em apoio à OTAN, as operações de HUMINT e CI tem de ser coordenadas e desconflituadas na máxima extensão possível entre os NIC e o CJ2X.

1019. Fluxo da Informação Adequada

- a. As responsabilidades dos elementos mencionados têm de ser definidas dependendo do tipo de missão, do facto do ambiente ser hostil ou amistoso no país hospedeiro e do tipo de ameaça existente/prevista. Poderão ser definidas da seguinte forma:
 - (1) Os elementos de CI, HUMINT e COMINT terão de ser avaliados. Deverá ser efectuada uma análise às notícias e às informações provenientes das suas

²¹ Elemento de Estado-Maior responsável por coordenar e desconflituar as missões a desempenhar pelo HUMINT e CI e num âmbito mais alargado à segurança, dentro da JOA e está subordinado ao CJ2. É também a entidade de ligação entre a Força e a Unidade de informações na AO.(AJP 2.3).

PDE 2-00 Informações, Contra-Informação e Segurança

próprias origens, órgãos, etc. na tentativa de encontrar eventuais ameaças no Teatro. A informação deverá ser transmitida imediatamente ao elemento de segurança no Teatro. Esta informação deverá ser a mais pormenorizada possível, para contrariar a ameaça, mas deve estar suficientemente bem expurgada (de acordo com as normas nacionais) para proteger a fonte e os meios de disseminação envolvidos.

- (2) O pessoal de Informações avaliará e analisará todas as origens abertas disponíveis no Teatro e todos os relatórios de informações recebidos. A informação relacionada com a FP CI/Segurança é transmitida ao J2X para ser colocada na base de dados central;
- (3) O J2X tem de monitorizar e relatar todas as actividades, intenções e capacidades relacionadas com a FP CI/Segurança. O pessoal de segurança em cooperação com o pessoal de informações²² é responsável por transmitir atempadamente avisos de ameaças, avaliações e propor acções aos comandantes e aos meios de FP no Teatro. O plano de segurança existente deverá ser revisto periodicamente ou se a situação assim o requerer.

- b. As mensagens de aviso, que chegarão aos comandantes responsáveis demasiado tarde devido a restrições de segurança ou de rotina e a meios de disseminação não adequados, não são utilizáveis. É da responsabilidade das células segurança envolvidas decidir qual a informação que pode ser filtrada para ser difundida. Compete também a estas células, difundir a informação atempadamente e decidir quais os meios de transmissão que deverão ser utilizados, de forma a contrariar a ameaça.

SECÇÃO VI – DISSEMINAÇÃO DA CONTRA-INFORMAÇÃO E SEGURANÇA

1020. Generalidades

A disseminação é a fase do Ciclo da Produção da Informação, na qual as informações são transmitidas àqueles que delas necessitam. Geralmente não existe uma diferença fundamental entre a disseminação de informações e os produtos da CI e Segurança. O factor tempo é um aspecto crítico na disseminação de todos os tipos de informações;

²² As responsabilidades entre as informações e o CI/Segurança diferem de uma nação para outra. Contudo, a FP é uma missão conjunta e a transmissão de avisos tem a primeira prioridade.

porém, o valor da CI e da segurança das informações pode sofrer uma degradação significativa ou perder mesmo utilidade, se chegar atrasada. Como todos os aspectos de segurança são da responsabilidade nacional, o estabelecimento de um sistema de disseminação de informação a nível internacional, é de vital importância. A disseminação pode ser oral, escrita, gráfica ou através da troca de dados.

1021. Relatórios

- a. Os briefings (orais) deverão:
 - Ser confinados a notícias e informações sobre actividades de serviços de informações hostis, grupos subversivos e terroristas, organizações e indivíduos, incidentes de segurança e falhas na segurança (se apropriado).
 - Seguir um modelo padrão.
 - Apresentar factos estabelecendo uma diferença clara entre estes e a interpretação dos mesmos, concluindo com uma estimativa das capacidades e intenções dos serviços de informações hostis, dos grupos subversivos/terroristas e das organizações ou indivíduos.
- b. Na forma escrita, os relatórios sobre CI e a segurança das informações deverão ser apresentados pelas seguintes formas:
 - Relatório de Contra-Informação e Segurança (CI/Security INTREP – *Intelligence Report*).
 - Relatório Suplementar de Contra-Informação e Segurança (CI/Security SUPINTREP– *Supplementary Intelligence Report*).
 - Sumário de Contra-Informação e Segurança (CI/Security INTSUM – *Intelligence Summary*).
 - Mensagens de Aviso de Contra-Informação e Segurança (CI/Security *Warning Messages*).
- c. Estes relatórios contêm notícias e informações sobre CI e Segurança. Os CI/Security INTREP deverão incluir uma descrição do incidente ou da actividade e a avaliação do seu significado. Os CI/Security INTSUM têm um conceito mais amplo e podem não incluir todos os incidentes ou actividades relatadas, mas têm obrigatoriamente de conter avaliações.

PDE 2-00 Informações, Contra-Inteligência e Segurança

- d. Adicionalmente, os órgãos nacionais e militares de CI e Segurança deverão fornecer, aos QG OTAN e forças aliadas, informações sobre a sua área de responsabilidade e deverão iniciar uma troca permanente e contínua de informações. Uma vez que os sistemas ADP, como CRONOS²³, BICES²⁴ ou LOCE²⁵ estão espalhados entre os QG OTAN, esta troca deverá ser efectuada em larga escala.

1022. Princípios da Disseminação da Contra-Inteligência e da Segurança

- a. A disseminação é a transmissão atempada de notícias ou informações, na forma adequada e através dos meios convenientes, àqueles que delas necessitem. No entanto, no que respeita à FP, os avisos deverão ser difundidos da forma mais abrangente possível, de modo a chegar a todas as unidades/militares das próprias forças ou de coligações que possam ser afectadas.
- b. Os Estados-Maiores de CI e Segurança são responsáveis por garantir que todas as notícias e informações são transmitidas a quem delas necessite, incluindo aos Estados-Maiores de CI e Segurança de unidades adjacentes.
- c. Os métodos de disseminação de relatórios e dados são definidos pela classificação da própria informação. Mas até mesmo a informação não classificada, deverá ser disseminada através de linhas de comunicação seguras, para assegurar que a mesma chegue ao destino. A *internet* não é um meio seguro para disseminar notícias e informações.
- d. O sucesso das medidas de segurança também dependerá da manutenção da ligação eficaz entre comandos autorizados e órgãos de CI e:
 - (1) Outros comandos militares nacionais e OTAN.
 - (2) Outros Estados-Maiores de CI e Segurança nacionais e OTAN.
 - (3) Autoridades de polícia local e alfândegas.
 - (4) Administração pública e outras autoridades civis.

²³ Crisis Response Operations in NATO Open Systems.

²⁴ Battlefield Information Collection and Exploitation Systems.

²⁵ Linked Operation-Intelligence Centres Europe.

- e. Em tempo de crise e de guerra, cada comando deverá encarregar os órgãos de ligação de estabelecer contacto com as unidades militares de outros países aliados e de assegurar o fluxo apropriado de notícias e informações. A ligação de segurança também deverá estabelecer o enquadramento necessário para uma fácil transição, das necessidades e actividades, do tempo de paz para o tempo de guerra.
- f. Com base na avaliação da ameaça fornecida pelos órgãos de segurança ou CI, os comandantes e chefes de órgãos em todos os escalões, estabelecerão medidas de segurança para neutralizar a ameaça. Adicionalmente, deverão assegurar a continuidade da instrução – que deverá ser dinâmica – variando na natureza e na forma para ir de encontro às alterações da ameaça.
- g. As CRO necessitam de um acesso rápido a uma Autoridade de Segurança para uma tomada de decisão operacional. Quando as forças da OTAN se encontram projectadas em CRO, as decisões operacionais podem ser necessárias no terreno. Para responder a estes requisitos, o SHAPE (*Supreme Headquarters Allied Powers Europe*) designará uma Autoridade de Segurança de Teatro, que exercerá uma vigilância diária sobre todos os aspectos do programa de segurança do comando e sobre as operações de CI, constituindo-se como o principal conselheiro do comandante em assuntos de CI, assim como o ponto de contacto para as Células Nacionais de Segurança no Teatro.

Página intencionalmente em branco

ANEXO A – PLANO DE PESQUISA

1. Plano de Pesquisa – MATRIZ (EXEMPLO)

(Classificação de Segurança)																
GDH: _____																
MISSÃO: _____																
Nº PIR (1)	CAPÍTULO PIR (2)	Nº IR o IR (3)	IR (4)	NAI TAI DP/DL (5)	Nº INDICADOR (6)	INDICADOR ou INDÍCIO TÉCNICO (7)	P R I O R I D A D E (8)	NET (9)	SEC TIOV (10)	E S T A D O (11)	ÓRGÃOS DE PESQUISA (12)				CAPÍTULO COOR DENAÇÕES (13)	R E L A T Ó R I O S (14)
											...	UAV	PAO	...		
...																
C	Irá o In atacar ao longo do Rio AZUL com mais de uma Divisão?	C-1	Meios de reconhecimento de Eng do In ao longo do rio AZUL.	DP 2	C-1-1	Reconhecimento de Eng na ponte de MIRA (GLG344647).		110930	120400Z				X			
				NAI 21	C-1-2	Reconhecimento de Eng nas proximidades de FRENO (GLG394467).		110930	120400Z			X				

(1) Numeração do PIR (de ordem alfabética).

(2) Descrição do PIR.

(3) Numeração da necessidade de informação (IR), de forma alfanumérica.

(4) Descrição da necessidade de informação (IR) ou quesitos concretos.

(5) Indicação do NAI, TAI ou DP/DL associado.

(6) Numeração do Indicador (de forma alfanumérica com base no IR a que se associa).

(7) Indicador ou indício técnico.

(8) Prioridade.

(9) Nunca antes de (NET).

(10) Tempo de validade da informação (LTIOV).

(11) Estado.

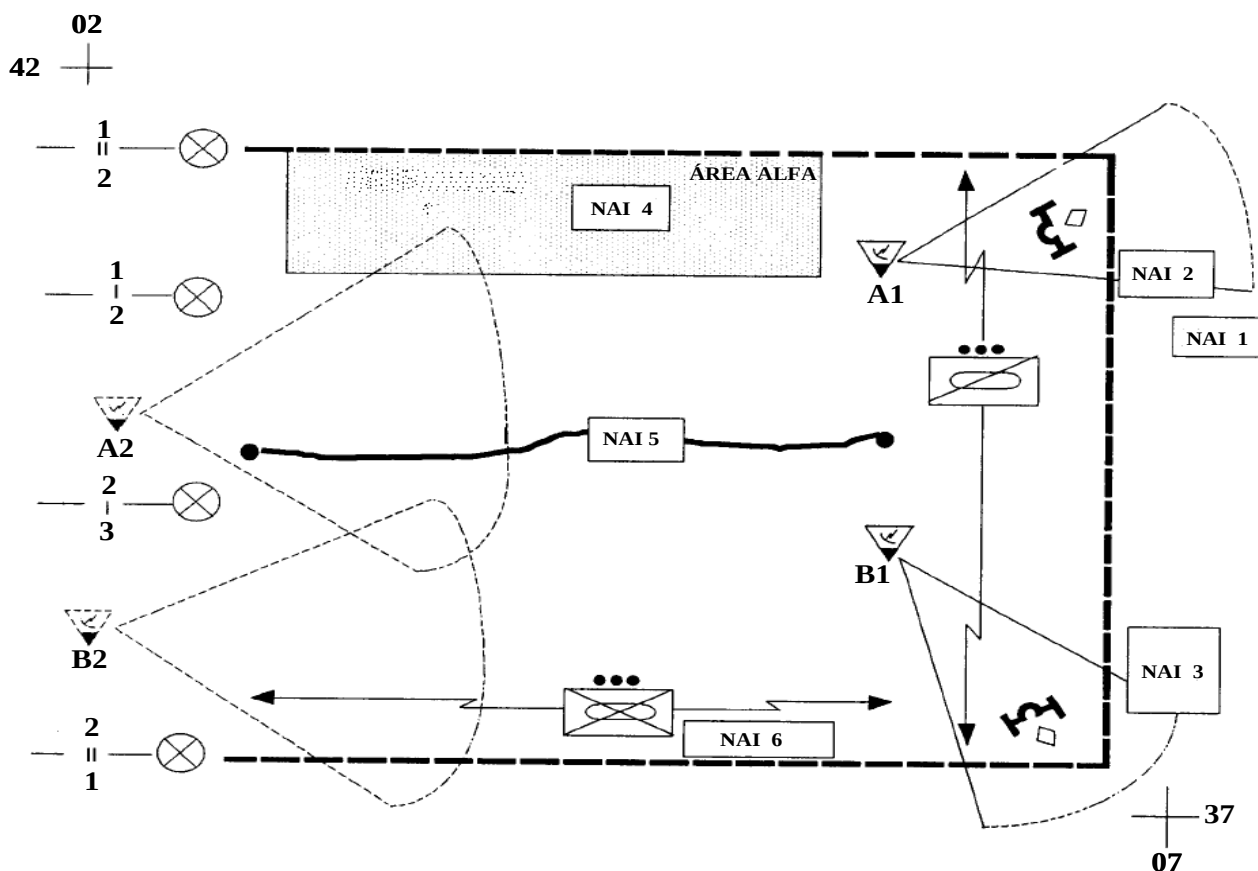
(12) Indicação do Órgão que vai executar a pesquisa.

(13) Coordenação a realizar.

(14) Relatórios associados.

(Classificação de Segurança)

2. Plano de Pesquisa – TRANSPARENTE (EXEMPLO)

**Instruções:**1 Cat:

Executa patrulhas de reconhecimento e segurança na Zona ALFA para detectar e alertar oportunamente patrulhas de Reconhecimento In apeadas e montadas.

Executar das patrulhas de reconhecimento e segurança entre ... e ... para detectar e alertar oportunamente patrulhas de Reconhecimento In apeadas e montadas à frente do seu Sector defensivo.

Monta PO/PE de acordo com NEP do Bat.

Relatórios de acordo com NEP do Bat.

2 Cat:

Executar das patrulhas de reconhecimento e segurança entre ... e ... para detectar e alertar oportunamente patrulhas de Reconhecimento In apeadas e montadas à frente do seu Sector defensivo.

Monta PO/PE de acordo com NEP do Bat.

(Classificação de Segurança)

Relatórios de acordo com NEP do Bat.

3 CAT:

Executar das patrulhas de reconhecimento e segurança para detectar e alertar oportunamente patrulhas de Reconhecimento In apeadas e montadas à frente do seu Sector defensivo.

Monta linha de vigilância NLT ... no flanco Sul do Sector defensivo do Bat para garantir o alerta oportuno da aproximação de

Monta PO/PE de acordo com NEP do Bat.

Relatórios de acordo com NEP do Bat.

PelRec:

Monta linha de vigilância NLT ... ao longo da linha definida pelas coordenadas ... para detectar Unidades de Reconhecimento In e impedir a sua acção de recolha de informação.

Coordenar com a 2ª CAT o itinerário para a posição de vigilância e com a SecVCB as posições de vigilância.

Relatórios de acordo com NEP do Bat.

SecVCB:

Ocupa posições A1 e B1 NLT alertar oportunamente a aproximação de Unidades de Reconhecimento In ao Sector do Bat.

Coordenar com ... a passagem de linha.

Coordenar com ... as posições a ocupar.

À ordem, ocupa as posições A2 e B2.

Relatórios de acordo com NEP do Bat.

Distribuição:

(Classificação de Segurança)

Página intencionalmente em branco

ANEXO B – ESTUDO DA SITUAÇÃO DE INFORMAÇÕES

1. ESTUDO DA SITUAÇÃO DE INFORMAÇÕES (MODELO)

(Classificação de Segurança)

Exemplar Nº __ de __ ex
Unidade
Local
Data e hora
Número de referência

ESTUDO DA SITUAÇÃO DE INFORMAÇÕES Nº __

Referências:

Cartas ou outros documentos

Além das actividades de produção de informações e a Preparação do Campo de Batalha pelas Informações vulgo IPB, que são actividades essenciais do OfInfo, este tem a responsabilidade para com o comandante de elaborar:

Definição:

O estudo de situação de informações consiste numa análise dos elementos relativos à área de operações e ao inimigo/ameaça, para determinar a influência que possam ter no cumprimento da missão

Então a finalidade do estudo de situação será analisar a influência dos elementos de **informação táctica** no cumprimento da missão (**condições meteorológicas, terreno e inimigo**).

MODELO (preconizado para o estudo)

1. MISSÃO
2. CARACTERÍSTICAS DA ÁREA DE OPERAÇÕES
3. SITUAÇÃO DO INIMIGO
4. POSSIBILIDADES DO INIMIGO
5. CONCLUSÕES

(Classificação de Segurança)

(Classificação de Segurança)

EstSITInfo/Un/Nº pag

1. MISSÃO

Enunciado da missão, tal como foi restabelecida pelo comandante. Se tiverem sido atribuídas prioridades ou finalidades intermédias, devem as mesmas ser também mencionadas.

2. CARACTERÍSTICAS DA ÁREA DE OPERAÇÕES

Este parágrafo visa determinar a influência das características da área de operações sobre as possibilidades do inimigo e sobre o cumprimento da nossa missão.

Deve conter, sempre, informações relativas ao clima, condições meteorológicas, efemérides e terreno. Normalmente para o oficial de informações de uma unidade de escalão inferior a Divisão, é suficiente considerar apenas a influência das condições meteorológicas e dos aspectos militares do terreno. Noutras circunstâncias, e quando possam afectar significativamente as operações de ambos os contendores, serão incluídas referências a condições políticas, económicas, sociais ou de qualquer outra natureza, respeitante à área ou à sua população.

a. Clima, Condições Meteorológicas, Efemérides e Outros Elementos

Descrição da situação prevista para o período em que devem ser realizadas as operações necessárias ao cumprimento da missão, no que respeita às condições meteorológicas e efemérides.

Incluir dados de luz e quaisquer previsões meteorológicas ou dados climáticos, conforme for apropriado. Utilizar anexos para informações pormenorizadas.

- (1) Condições Meteorológicas
- (2) Efemérides
- (3) Influência Sobre as Possibilidades do Inimigo
- (4) Estudo dos efeitos do factor em causa sobre as possibilidades do inimigo.
- (5) Influência Sobre o Cumprimento da Nossa Missão
- (6) Estudo dos efeitos do factor em causa sobre operações a realizar pelas nossas forças, para cumprirem a missão.

(Classificação de Segurança)

Neste parágrafo analisa-se o modo como o **clima** as **condições meteorológicas** e as **efemérides**, influenciam o cumprimento das possibilidades do **IN** e o **cumprimento da nossa missão**

No clima inclui-se um **sumário climático** e **dados de temperatura** (recebem-se do escalão superior)

Nas **condições meteorológicas** inclui-se os elementos definidores tais como:

- Precipitação
- Nevoeiro
- Nebulosidade
- Humidade relativa
- Pressão atmosférica
- Vento

VISIBILIDADE:

Pode ser limitada pelo nevoeiro, nebulosidade, precipitação, fumos e dados de luz.

A eficácia dos PO/PE é afectada pelas más condições meteorológicas.

Os radares são afectados pela chuva e nevoeiros, que causam confusão ao operador.

Afecta o comando e controlo, segurança, apoio de fogos (aéreos e terrestres), a cobertura de movimentos, possibilidade de decepção e surpresa.

Quando é reduzida favorece o atacante por:

- Conferir cobertura;
- Reduzir a eficácia dos fogos do defensor;
- Possibilitar a aproximação de surpresa;
- Prejudicar se o ataque exigir grande apoio aéreo e fogos observados.

TRAFICABILIDADE:

É afectada pela precipitação, temperatura e natureza dos solos.

PESSOAL E EQUIPAMENTO:

Só é afectado em condições extremas.

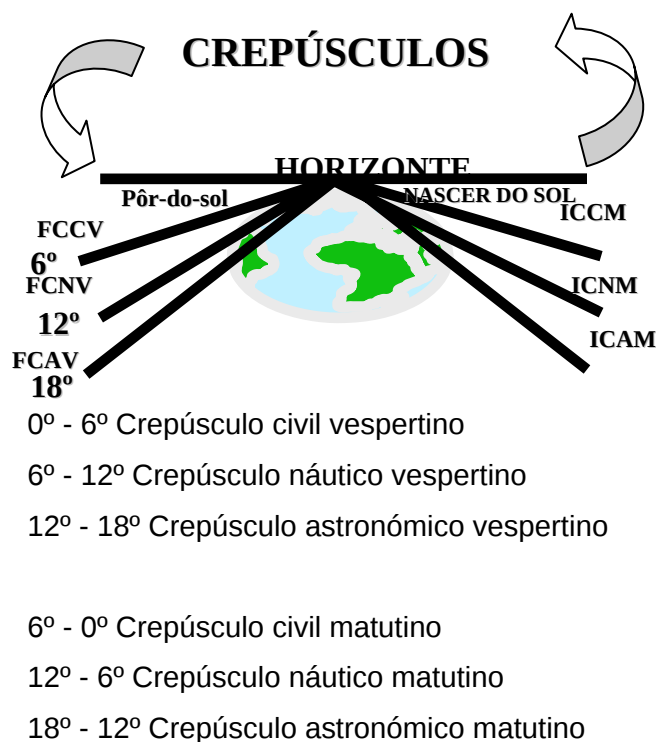
(Classificação de Segurança)

EstSITInfo/Un/Nº pag

UTILIZAÇÃO DE FUMOS E NBQ:

A influência mais importante é sem dúvida a direcção e velocidade do vento.

- **Fumos** – ventos fracos e moderados (5 a 16Km/h)
- A direcção ideal é quando o vento sopra em direcção paralela à frente IN
- **NBCR** – 1 a 2 nós/h para criação de zonas contaminadas estacionárias, pode ir até aos 6 nós/h (nó=1,85km/h)
- A direcção ideal é quando o vento sopra nas costas de quem utiliza as armas NBCR

EFEMÉRIDES:

Os almanaques ou folhetos de dados astronómicos publicados pelos organismos civis não contêm ou não referem segundo a terminologia aplicável a fins militares.

Normalmente utilizam-se as designações de:

- Raiar da aurora – ICAM
- Dia claro – ICCM

(Classificação de Segurança)

- Nascer do sol – ICCM
- Por do sol
- Escurecer – ICCM
- Noite fechada – FCC

DEFINIÇÕES:**Início Crepúsculo Astronómico Matutino (ICAM) /Raia da Aurora**

O Sol encontra-se antes do seu nascimento a 18º abaixo do horizonte.

Final da completa escuridão.

Início Crepúsculo Náutico Matutino (ICNM)

Hora a partir da qual há possibilidade de coordenação próxima entre unidades de pequenos efectivos Sol encontra-se 12º abaixo horizonte.

Início Crepúsculo Civil Matutino (ICCM) /Dia Claro

O Sol encontra-se 6º abaixo horizonte. Desaparecimento de estrelas de 1ª Grandeza.

Final Crepúsculo Civil Vespertino (FCCV) /Escurecer

O Sol encontra-se 6º abaixo do horizonte. Caracteriza-se pelo aparecimento de estrelas de 1ª grandeza.

Final Crepúsculo Náutico Vespertino (FCNV)

Hora partir qual deixa haver possibilidade coordenação próxima entre unidades. Sol encontra-se 12º abaixo horizonte.

Final Crepúsculo Astronómico Vespertino (FCAV) /Noite Fechada

Sol encontra-se 18º abaixo horizonte. Começo completa escuridão

Entre o ICCM e o Nascer do Sol – Hora a partir qual é possível regular fogos apoio.

Entre o Pôr-do-sol e o FCCV – Hora a partir qual deixa ser possível regular fogos apoio.

Hora H – Deve coincidir com hora partir da qual é possível regular fogos.

b. Terreno**(1) Situação**

Utilizar representações gráficas, quando possível, e anexos para assuntos detalhados. Incluir as informações estritamente necessárias a uma boa compreensão dos pontos relativos a observação e campos de tiro, cobertos e abrigos, obstáculos, pontos importantes do terreno e eixos de aproximação. Incluir os efeitos de cada um destes

(Classificação de Segurança)

factores, sobre o emprego de armas nucleares, agentes químicos e biológicos, e quaisquer outras considerações pertinentes, quando apropriado.

(a) Descrição geral da área

1. Relevo e hidrografia
2. Vegetação
3. Natureza do solo
4. Alterações resultantes da acção do homem

(b) Aspectos militares da área

1. Observação e campos de tiro
2. Cobertos e abrigos
3. Obstáculos
4. Pontos importantes
5. Eixos de aproximação

(2) Influência Sobre as Possibilidades do Inimigo

Discutir de forma idêntica à indicada para os factores mencionados em 2.a.(2). No estudo da possibilidade de defesa, indicar a melhor área de defesa e os melhores eixos de aproximação que conduzam aquela área.

Para a possibilidade de ataque, referir os melhores eixos de aproximação que o inimigo pode utilizar.

(3) Influência Sobre o Cumprimento da Nossa Missão

Discutir de forma idêntica ao preconizado na alínea 2.a.(3).

c. Outras Características

As seguintes características adicionais são consideradas, quando pertinentes, em subparágrafos distintos: sociologia, política, economia, psicologia e outras. Outros factores podem incluir assuntos como ciência, materiais, transportes e potencial humano. Estes factores são analisados à luz das condições meteorológicas e do terreno. Se necessário constarão em anexo.

(Classificação de Segurança)

Descrição geral da área

Neste ponto é abordado o **terreno**, e a forma como **influência** as possibilidades do IN e o cumprimento da nossa missão;

Relevo e hidrografia

Definir uma imagem do aspecto geral do terreno

Definir a sua compartimentação (transversal ou longitudinal)

Conceito associado:

Compartimento de terreno é uma zona limitada, pelo menos lateralmente, por acidentes que impedem a observação e a execução de fogos directos para o seu interior, a partir de pontos exteriores ao compartimento.

Definir rios e linhas de água existentes, tendo em conta a sua largura e profundidade e natureza das margens.

Vegetação

Verificar a existência de terrenos cultivados e ou arborizados, e neste caso definir a natureza e porte das árvores existentes e extensão das matas.

Natureza do solo

Se tem ou não influência na progressão das tropas e caminhos existentes, e neste caso definir a sua classificação, forma como corta a AOp e como são influenciados pelas condições meteo.

Alterações resultantes da acção do homem

Existência de povoações (nomes e dimensões).

Definir a existência de estradas e respectiva classificação (X, Y e Z), e a forma como cortam a AOp.

Definir a existência de pontes, represas, muros, aramados, etc

Aspectos militares da área

Observação e campos de tiro

Conceitos associados:

A **Observação** relaciona-se com a influência do terreno na aptidão de uma força para vigiar uma determinada área, quer visualmente, quer através do emprego de meios de vigilância.

Os **Campos de Tiro** compreendem o estudo da influência do terreno na eficácia dos fogos das armas de tiro directo e indirecto.

Na análise das possibilidades gerais de **observação** – terrestre e aérea – que se deparam tanto às nossas tropas como ao IN, há que atender à influência das condições meteorológicas, relevo vegetação e alterações resultantes da acção do homem. Neste ponto devem estar incluído a capacidade de ver o IN por intermédio de dispositivos electrónicos ou por outros processos ópticos

Cobertos e abrigos

Conceitos associados:

Os Cobertos conferem protecção contra a observação; os Abrigos conferem protecção contra fogos.

Como corolário do ponto **Cobertos e abrigos**, podemos dizer que as unidades procuram constantemente terreno com cobertura e abrigos para as suas tropas e que dessas posições possam concentrar os seus fogos sobre forças do IN que se desloquem em terreno que não ofereça qualquer cobertura e abrigo.

Obstáculos

Conceito associado:

Obstáculo, é algo natural ou artificial que impede, retarda e canaliza o movimento de unidades militares.

Pontos importantes

Conceito associado:

Um Ponto Importante é todo o local ou área cujo controlo confere uma nítida vantagem a qualquer das forças (NT ou IN). A escolha de um Ponto Importante varia com o Escalão, tipo e missão da Unidade.

Eixos de aproximação

Um Eixo de Aproximação é uma faixa de terreno que uma força de um determinado Escalão pode utilizar para alcançar um Objectivo ou Ponto Importante.

Para ser considerado Eixo de Aproximação, esta faixa de terreno deve ter **espaço suficiente** para o emprego, no mínimo, de uma unidade de manobra de **escalão adequado**.

3. SITUAÇÃO DO INIMIGO

Neste número incluem-se as informações sobre o inimigo que mais tarde permitirão deduzir as suas possibilidades e vulnerabilidades e concluir por uma modalidade de acção e sua probabilidade relativa de adopção.

a. Dispositivo

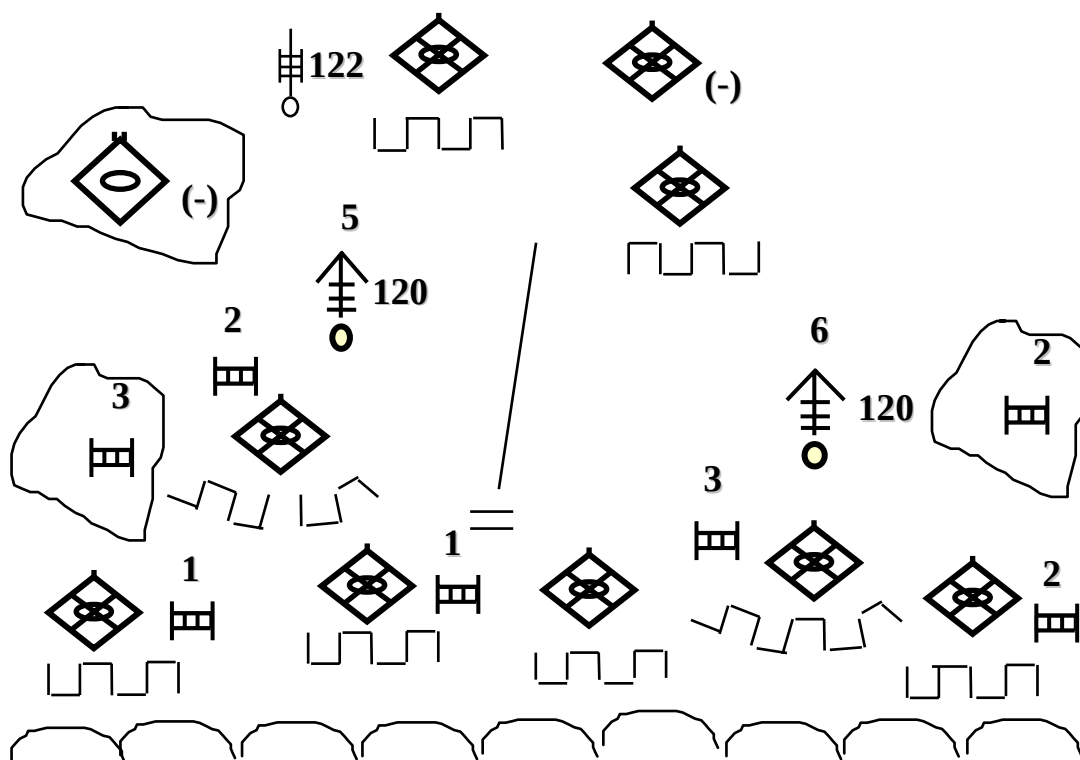
Normalmente, é indicado sob a forma gráfica, numa carta ou transparente, ou fazendo referência a qualquer documento publicado.

(Classificação de Segurança)

EstSITInfo/Un/Nº pag

No dispositivo geralmente faz-se referência ao seguinte:

- Ao transparente de situação;
- Localização e desenvolvimento tático das forças inimigas, incluindo como aproveitam o terreno (em **trincheiras**, em movimento, **desenvolvimento**, em **ZRn**);
- Analisar o dispositivo por faixas, primeiro na globalidade um escalão acima (verificar se estão em frentes normais ou extensas);
- Representar o IN considerando **dois escalões abaixo**.



b. Composição

Sumário da ordem de batalha das forças que se nos opõem e outras forças inimigas que podem afectar o cumprimento da missão. Serve de base à posterior determinação do potencial que o inimigo pode empregar contra as nossas forças. Abrange a organização estrutural (Infantaria, Blindados, etc.), a identificação específica das unidades inimigas e outras informações da ordem de batalha.

Pode fazer-se referência a documentos previamente difundidos. É feita menção especial a unidades de Guerra Electrónica, forças de guerrilha ou de operações especiais, se apropriado.

(Classificação de Segurança)

Neste paragrafo, a composição divide-se em:**Identificação**

- Escalão
- Tipo de unidade (arma/svc)
- Designação numérica ou nominal
- Cmd de que depende (Un e escalão acima)

Organização estrutural

- Estrutura da unidade
- Posicionamento dos diversos escalões

Outras informações da OB

- Forças de guerrilha
- Un apoio aéreo
- De lançamentos de meios aéreos
- Guerra electrónica

c. Potencial de Combate

São mencionadas todas as unidades inimigas que, admissivelmente, podem ser empregues contra a nossa unidade de forma a afectar o cumprimento da missão.

O potencial de combate deve ser estudado e descrito em termos de forças empenhadas, reforços e possibilidades aéreas, nucleares, biológicas, químicas e radiológicas como a seguir se refere. A finalidade desta articulação é contribuir para o desenvolvimento de possibilidades e vulnerabilidades do inimigo que permitam ao comandante e estado-maior a selecção de modalidades de acção.

(1) Forças Empenhadas

São consideradas forças empenhadas as unidades tácticas em contacto e as respectivas unidades de apoio de fogos cujo emprego em áreas diferentes daquelas que ocupam, não é, logicamente, de admitir.

(Classificação de Segurança)

EstSitiInfo/Un/Nº pag

Aquelas unidades tácticas são expressas em termos de dois escalões imediatamente abaixo daquele em que é feito o estudo.

A designação das forças inimigas como forças empenhadas depende, primariamente, do seu dispositivo, localização e escalão em que o estudo está a ser feito.

Em caso de dúvida sobre se uma unidade deve ser considerada como empenhada ou reforço, deve admitir-se como reforço.

(2) Reforços

São considerados reforços todas as forças inimigas que não estejam empenhadas contra a unidade cujo comando realiza o estudo, ou contra quaisquer outras forças amigas e que possam, razoavelmente ser consideradas em condições de intervir em tempo oportuno na zona de acção daquela unidade de forma a afectarem o cumprimento da missão.

Os reforços são indicados da forma que for mais conveniente. Dispositivo, localização, escalão de controlo ou outros factores considerados no momento do estudo, permitem a determinação das forças inimigas que devem ser consideradas como reforços.

(3) Apoio Aéreo

São considerados o número e tipo de saídas diárias que o inimigo pode efectuar contra a unidade. Na impossibilidade de avaliação das possibilidades do inimigo no que concerne à Unidade que elabora o estudo, são consideradas as possibilidades inimigas formuladas pelo escalão superior.

(4) Apoio NBQR

A determinação das possibilidades NBQR do inimigo, baseia-se, normalmente, na estimativa do número e tipo de armas e das disponibilidades e tipo de agentes, bem como no conhecimento da doutrina do inimigo, na experiência adquirida e no estudo das possibilidades do inimigo.

Conforme se deixou anotado para o apoio aéreo, também no apoio NBQR são, normalmente, consideradas as possibilidades inimigas formuladas pelo escalão superior.

d. Actividade Recente e Actual

Resume a actividade inimiga, recente e em curso, que possa revelar quais as suas acções futuras e também qualquer incapacidade significativa do inimigo para levar a cabo determinadas actividades.

(Classificação de Segurança)

e. Aspectos Característicos e Pontos Fracos

Baseado no conhecimento da doutrina tática do inimigo, procedimentos, princípios da guerra, área de operações e situação do inimigo, previamente descritos e discutidos, expor os aspectos característicos e pontos fracos para posteriormente deduzir as vulnerabilidades do inimigo que possam ser exploradas. Os dados expostos são agrupados em subparágrafos que a seguir se indicam. Apenas se utilizam os subparágrafos julgados pertinentes.

(1) Pessoal

1. Moral e eficiência para o combate (ser inferior a excelente);
2. Elevada percentagem de combatentes excessivamente novos ou velhos;
3. Fraco nível sanitário;
4. Percentagem dos efectivos orgânicos (Se inferior a 80%);
5. Deficiências notórias no serviço de reabastecimento (Em particular especialistas).

(2) Informações

- (a) Facilidade de decepção ou neutralização de órgãos de pesquisa IN;
- (b) Excessiva dependência de uma ou mais origens de notícias;
- (c) Ineficiência do seu SIM.

(3) Operações

Normalmente inclui-se um estudo sobre a eficiência de combate, se inferior a excelente.

- (a) Repetição sistemática de certos esquemas de manobra;
- (b) Deficiente organização do terreno;
- (c) Deficiente colocação das reservas;
- (d) Deficiente grau de instrução;
- (e) Falta de mobilidade;
- (f) Onde têm os seus limites;
- (g) Posições das armas.

(4) Logística

- (a) Se se verificar fraqueza aparente, incluir um estudo sobre a capacidade do inimigo para apoiar logisticamente as suas forças.
- (b) Falta de determinados abastecimentos ou material

(Classificação de Segurança)

EstSitInfo/Un/Nº pag

- (c) Percentagem estimada do equipamento orgânico (Se inferior a 80%)
- (d) Excessiva concentração dos órgãos de reabastecimento
- (e) Incapacidade para proceder ao reabastecimento durante as operações
- (5) CIMIC
 - É feita, normalmente, uma avaliação sobre a atitude da população civil e existência de alimentos, abastecimentos, condições sanitárias e comunicações.
- (6) Personalidades
 - Incluir, normalmente, um estudo das capacidades e/ou fraquezas dos comandantes e oficiais do estado-maior das principais unidades inimigas.
 - (a) Personalidade dos Cmdt e EM IN;
 - (b) Competência profissional e experiência;
 - (c) Outros aspectos relevantes do Cmdt e EM IN.

4. POSSIBILIDADES DO INIMIGO

São as manobras que o inimigo é materialmente capaz de executar e que, se forem adoptadas, afectarão o cumprimento da nossa missão. Com base em todas as informações prévias e estudos, desenvolver e expor as possibilidades do inimigo.

A sua análise permitirá deduzir as manobras que o inimigo pode adoptar e a sua probabilidade relativa de adopção.

a. Enumeração

Constitui uma lista de possibilidades atribuídas ao inimigo, com base no seu dispositivo, composição e potencial de combate. Para cada possibilidade indicar O QUÊ, QUANDO, ONDE e COM QUE MEIOS.

b. Análise e Estudo

Cada possibilidade, ou combinação apropriada de possibilidades, é discutida em alíneas independentes, face aos indicadores ou indícios técnicos que surgirem da adopção ou rejeição pelo inimigo de cada uma das possibilidades atribuídas. Se uma determinada possibilidade é particularmente perigosa para o cumprimento da missão das nossas forças, essa possibilidade deve ser sempre salientada, mesmo que não haja qualquer indício sobre a sua possível adopção.

(Classificação de Segurança)

A apreciação é realizada sempre do ponto de vista do IN, além dos indícios considerar:

- (1) Doutrina e formas de actuação;
- (2) Consequências que para o IN podem advir, pela adopção ou rejeição de cada possibilidade.

5. **CONCLUSÕES**

Contém a interpretação final do oficial de informações, a qual refere a influência das condições meteorológicas, do terreno e do inimigo no cumprimento da missão da unidade. Assim, as conclusões indicam a influência global das características da área de operações nas modalidades de acção das nossas forças, as possibilidades do inimigo mais prováveis incluindo a sua probabilidade relativa de adopção e as suas vulnerabilidades. Estas considerações permitem seleccionar modalidades de acção.

a. Influência das Características da Área de Operações Sobre o Cumprimento da Nossa Missão

Refere os efeitos das características da área de operações nas modalidades de acção que permitem ou facilitam o cumprimento da missão.

Para modalidades de acção de ataque, indicar os melhores eixos de aproximação. Quer na defesa quer no ataque assim sendo:

(1) Defesa

- a. Melhores áreas de defesa;
- b. Melhor eixo de aproximação do IN para a nossa posição.

(2) Ataque

- a. Melhores áreas de defesa utilizáveis pelo IN;
- b. Melhor eixo de aproximação para as NT atingirem o objectivo.

b. Probabilidade Relativa de Adopção das Possibilidades do Inimigo

As possibilidades são relacionadas por ordem da sua probabilidade relativa de adopção.

A relação poderá incluir possibilidades subordinadas que podem ser adoptadas concorrentemente. Normalmente, apenas duas ou três possibilidades, tendo em vista a determinação da probabilidade relativa de adopção, podem ser justificadas pelos indicadores ou indícios técnicos disponíveis.

(Classificação de Segurança)

EstSitInfo/Un/Nº pag

A probabilidade relativa de adopção das possibilidades do inimigo deve sintetizar várias possibilidades numa só, a fim de se obter uma maior clareza e concisão. No entanto tal só será possível se as possibilidades que se reúnem puderem ser todas concretizadas de uma forma concorrente, numa manobra lógica e conjugada a executar pelo inimigo.

Tenha-se em atenção que no caso da manobra inimiga mais provável não ser a mais perigosa para o cumprimento da nossa missão, se deve mencionar e indicar, sempre, a manobra que se considera mais perigosa.

c. Vulnerabilidades do Inimigo

Referir as influências dos aspectos característicos e pontos fracos que resultam em vulnerabilidades e que podem ser exploradas. A ordem da relação destas vulnerabilidades é arbitrária.

- (1) Localização do PC;
- (2) ZRn;
- (3) Limites;
- (4) Locais de reabastecimento;
- (5) Armas de Apoio;
- (6) Conhecimento de unidades de efectivo reduzido;
- (7) Mau aproveitamento do terreno;
- (8) Flancos expostos;
- (9) Frentes extensas;
- (10) Locais de deficiente apoio mútuo;
- (11) Dificuldades de reabastecimento.

(Acusar a recepção)

O Comandante

(nome)
(posto)

Autenticação:
O Chefe da 2ª Rep

(nome)
(posto)

Anexos:

Distribuição:

(Classificação de Segurança)

ANEXO C – ANEXO DE INFORMAÇÕES

1. ANEXO DE INFORMAÇÕES (MODELO)

(Classificação de Segurança)

Exemplar N.º ___ de ___ ex

Unidade

Local

Data e hora

Número de referência

Anexo ___ (INFORMAÇÕES) à OOp ___

Referências:

1. SUMÁRIO DA SITUAÇÃO DO INIMIGO

(Pode figurar em apêndice)

- a. Resumo das informações essenciais à operação a que o anexo diz respeito, ou referência a qualquer apêndice ou documento se aqueles elementos tiveram sido já distribuídos a todas as unidades a quem o anexo se destina.
- b. Impressão do comandante sobre o inimigo ou, simplesmente a probabilidade relativa de adoção das possibilidades do inimigo.

2. NECESSIDADES PRIORITÁRIAS DE INFORMAÇÕES

Pode constar de um plano de informações táticas em apêndice.

Contém as necessidades prioritárias de informações (PIR – *Priority Intelligence Requirements*) constantes do Plano de Pesquisa referentes à operação em questão.

3. NECESSIDADES DE INFORMAÇÃO

Contém as necessidades de informação (IR – *Information Requirements*) constantes do Plano de Pesquisa referentes à operação em questão.

(Classificação de Segurança)

(Classificação de Segurança)

4. **MISSÕES DE PESQUISA**

É o parágrafo mais importante do anexo por conter indicações das notícias a pesquisar, pelos vários órgãos disponíveis, com a finalidade de confirmar ou não as necessidades prioritárias de informações.

Aqui, confirmam-se ou cancelam-se ordens ou pedidos de pesquisa do anteriormente expedidos. Este parágrafo compreende as ordens às unidades subordinadas e de reforço e os pedidos aos escalões superior, vizinhos e de apoio.

Este parágrafo contém dois subparágrafos:

a. Ordens às Unidades Subordinadas e de Reforço

As unidades são mencionadas pela ordem em que figuram no parágrafo 3. EXECUÇÃO da Ordem ou Plano de Operações

b. Pedidos aos Escalões Superior, Vizinhos e de Apoio

Procede-se de maneira semelhante ao indicado para as ordens de pesquisa a enviar às unidades subordinadas e de reforço.

5. **PESSOAL, DOCUMENTOS E MATERIAL CAPTURADOS**

Normalmente em NEP, pelo que neste parágrafo são indicadas apenas as alterações exigidas pela situação particular do momento.

a. Pessoal

Trata de instruções relativas a prisioneiros de guerra, desertores, repatriados, expatriados e população civil, em geral. É elaborado depois de um entendimento com os oficiais de Pessoal, Logística e CIMIC.

b. Documentos Capturados

Contém normas ou instruções para manuseamento, estudo e encaminhamento. Pode incluir instruções sobre pesquisa de documentos de tipo especial.

c. Material Capturado

Contém normas ou instruções sobre tipo, manuseamento e entrega de material inimigo capturado.

Elaborado após coordenação com o oficial de Logística e Serviços interessados.

(Classificação de Segurança)

6. ATRIBUIÇÃO E REQUISICÃO DE DOCUMENTOS E MATERIAL

Contém indicações sobre as condições em que são atribuídos às unidades ou por estas requisitadas, documentos ou material de informações.

Normalmente remete-se para NEP.

7. CONTRA-INFORMAÇÃO

Contém as medidas de contra-informação que, por serem específicas da operação, não constam das NEP respectivas.

Quando for grande o volume ou tecnicismo daquelas medidas, é redigido um apêndice de contra-informação.

Todas as determinações de interesse geral, como por exemplo, restrições aos reconhecimentos ou limitações no uso de meios rádio, embora citadas neste parágrafo ou no apêndice de contra-informação, são sempre repetidas no corpo da ordem ou plano de operações.

8. RELATÓRIOS E SUA DISTRIBUIÇÃO

Podem constar em NEP. Se houver alterações, referem-se as condições que regulam a disseminação de documentos de informações pelo comando que elabora o anexo, durante o período da operação.

(Classificação de Segurança)

Anx __/OOp __/Un/Nº pag

9. DIVERSOS

Neste parágrafo indicam-se, eventualmente, instruções necessárias, não incluídas nos parágrafos anteriores, nas NEP, ou exigindo procedimento diferente do estabelecido nestas.

(Acusar a recepção)

O Comandante

(nome)

(posto)

Autenticação:

O Chefe da 2ª Rep

(nome)

(posto)

Apêndices:

Pode englobar: sumário da situação do inimigo, plano de informações táticas, plano de vigilância, plano de patrulha, plano de reconhecimento aéreo, plano da contra-informação, etc.

Distribuição:

(Classificação de Segurança)

GLOSSÁRIO DE TERMOS E DEFINIÇÕES

ADVERSÁRIO

Refere-se a uma entidade, grupo ou força identificada como hostil às nossas forças e em que a aplicação da força pode estar prevista. Não existe uma declaração de guerra oficial (AAP 6).

ANÁLISE

É um passo da fase de Processamento do Ciclo da Produção da Informação que consiste em determinar e isolar os elementos significativos da notícia, para subsequente interpretação.

ANEXO DE INFORMAÇÕES

É um documento de disseminação de informações e transmissão de instruções relativas às actividades de informações visando uma determinada operação. Este documento constitui o processo formal de pôr em execução o plano de pesquisa. É distribuído normalmente como anexo a um plano ou ordem de operações.

AQUISIÇÃO DE OBJECTIVOS

É definida, em termos de ISTAR, como a detecção, identificação e localização de um objectivo, de forma suficientemente detalhada que permita o emprego efectivo de armas de fogos directos e indirectos.

ÁREA DESIGNADA DE INTERESSE (NAI)

Local onde possam ocorrer acontecimentos de importância para a condução da operação.

ÁREA DE INTERESSE (AOI)

A AOI pode ser definida como a área de preocupação de um comandante, para além da AOO, onde a existência de factos e acontecimentos ou a provável ocorrência de actividades possam vir a afectar as operações correntes ou futuras. Caso não consiga obter essas informações com os seus meios de pesquisa, terá que as solicitar ao escalão superior ou às unidades adjacentes. As notícias e informações obtidas fora da AIR devem ser disseminadas para todas as unidades a quem possam interessar. A AOI pode ser definida em termos de espaço e tempo.

ÁREA DE OBJECTIVO DE INTERESSE (TAI)

É o local onde o comandante pode influenciar a operação ao destruir, retardar ou desorganizar a ameaça, utilizando os seus meios de ataque, como por exemplo reservas, artilharia e apoio aéreo.

ÁREA DE OPERAÇÕES (AOO)

É uma área definida pelo comandante das forças conjuntas para as forças terrestres e navais para conduzir as operações militares e para a administração dessas operações. Normalmente, as áreas de operações não envolvem toda a área operacional do comandante das forças conjuntas, mas devem ser suficientemente extensas para permitir aos comandantes de componente o cumprimento da missão e a protecção da força.

ÁREA DE OPERAÇÕES CONJUNTAS (JOA)

É a porção de espaço terrestre, marítimo e aéreo definido por um comandante estratégico, em coordenação com as nações e aprovada pelo NAC/MC, e em concordância com a arquitectura de planeamento operacional da NATO, e na qual um determinado comandante conjunto planeia e conduz operações militares com vista ao cumprimento de uma missão específica. A JOA e os seus parâmetros definidores tais como tempo, âmbito e área geográfica variam de acordo com a missão ou contingência e pode sobrepor-se às áreas de responsabilidade.

ÁREA DE RESPONSABILIDADE DE INFORMAÇÕES (AIR)

É definida como a área geográfica atribuída a um comandante, na qual este é o responsável pela obtenção de informações, de acordo com os meios à sua disposição. Na prática, a dimensão desta área será limitada pelas capacidades dos meios de pesquisa à sua disposição, das quais o alcance e acesso serão os principais factores. Ambos os factores influenciarão a área na qual o comandante orientará o esforço da célula de informações.

ARQUITECTURA DAS INFORMAÇÕES NA OTAN

Consiste nas organizações, processos e sistemas interligados de órgãos de pesquisa, bases de dados, aplicações, produtores e utilizadores de informações.

AVALIAÇÃO

É um dos passos da fase de Processamento do Ciclo da Produção da Informação que consiste na apreciação de um item de informação relativamente ao grau de confiança da origem ou órgão de pesquisa e ao grau de verosimilhança da notícia.

AVALIAÇÃO DOS DANOS NO ESPAÇO DE BATALHA (BDA)

É a avaliação exacta e oportuna dos efeitos de uma aplicação da força letal ou não-letal contra um objectivo pré-determinado.

AVALIAÇÃO DA SITUAÇÃO (SA)

É a compreensão do ambiente operacional no contexto da missão do comandante.

CICLO DA PRODUÇÃO DA INFORMAÇÃO

O Ciclo da Produção da Informação é uma sequência das actividades de informações na qual a notícia é obtida, transformada em informação e explorada. Esta sequência compreende quatro fases distintas (orientação do esforço de pesquisa, pesquisa, processamento e disseminação) que culmina na distribuição do produto acabado.

CICLO DE TARGETING

É o mecanismo através do qual os produtos do sistema ISTAR são inter-ligados aos meios ofensivos, de forma a assegurar que é utilizado o sistema de armas mais adequado, ou outra capacidade, para atacar cada objectivo.

CONCEITO DE OPERAÇÃO (CONOPS)

Declaração clara e concisa sobre a linha de acção escolhida por um comandante de modo a cumprir a sua missão.

CONTRA-INFORMAÇÃO (CI)

A CI é definida como o conjunto de actividades relacionadas com a identificação e neutralização da ameaça à segurança, constituída por serviços de informações e organizações hostis ou por indivíduos relacionados com espionagem, sabotagem, subversão ou terrorismo.

CONTRA-TERRORISMO (CT)

É o conjunto de actividades relacionadas com a identificação e neutralização da ameaça à segurança, constituída por serviços de informações e organizações hostis ou por indivíduos relacionados com espionagem, sabotagem, subversão ou terrorismo.

CRIME ORGANIZADO

O crime organizado pode ser descrito como as acções de organizações de natureza criminosa, estruturadas em rede, com um ou mais líderes e várias unidades subordinadas espalhadas num vasto território.

DIRECÇÃO

Em termos de Informações, o mesmo que Orientação do Esforço de Pesquisa.

DISSEMINAÇÃO

É definida como a disponibilização oportuna de uma notícia ou informação, numa forma apropriada e através de meios adequados, àqueles que delas necessitam.

ELEMENTOS ESSENCIAIS DE INFORMAÇÃO DAS FORÇAS AMIGAS (EEFI)

São os aspectos fundamentais de uma força amiga que, se forem conhecidos do inimigo, comprometem o cumprimento de uma missão, tendo de ser protegidos da pesquisa inimiga; ou seja, como é que se pode evitar que a força inimiga nos veja.

ESPIONAGEM

A espionagem pode ser descrita como um método utilizado pelos serviços de informações hostis, para obter informação que afecte a segurança nacional, à qual não têm direito.

ESTUDO CONJUNTO DO ESPAÇO DE BATALHA PELAS INFORMAÇÕES (JIPB)

É uma metodologia gráfica analítica que é conduzida por células de informações conjuntas para produzir avaliações de informações, estudos da situação e outros produtos de informações em proveito do processo da decisão do comandante da força.

ESTUDO DO ESPAÇO DE BATALHA PELAS INFORMAÇÕES (IPB)

É um processo de análise da ameaça e do ambiente operacional, executado de uma forma sistemática e contínua, numa área geográfica específica que serve para apoiar o processo de decisão e os estudos do estado-maior.

ESTUDO DA SITUAÇÃO DE INFORMAÇÕES

Documento escrito que, tendo como elemento orientador a missão, analisa os aspectos mais característicos da área de operações e da situação do inimigo, com vista a deduzir a influência destes factores no cumprimento da missão e das modalidades de acção do inimigo e suas vulnerabilidades. Difere do IPB por se tratar de um documento escrito, enquanto aquele é apresentado de forma gráfica.

EXPLORAÇÃO DE DOCUMENTOS (DOCEX)

Extracção sistemática de notícias, em todos os formatos media, na resposta às necessidades de pesquisa.

FONTES

O mesmo que origens de notícias.

GESTÃO DAS NECESSIDADES DE INFORMAÇÕES E COORDENAÇÃO DA PESQUISA (CCIRM)

A CCIRM é o processo de gestão da pesquisa e é definida como o processo de converter necessidades de informações em necessidades de pesquisa; estabelecer, atribuir ou coordenar acções com origens ou órgãos de pesquisa adequados; monitorizar resultados e reatribuir acções de acordo com as necessidades.

Engloba aquelas actividades que resultam num emprego eficiente e eficaz da pesquisa, processamento, exploração e disseminação de informações para satisfazer as necessidades de informações aos níveis tático, operacional e estratégico e nacional. A CCIRM compreende dois componentes principais: a coordenação da pesquisa e a gestão das necessidades de informações que resultam de operações ou missões.

IMAGEM OPERACIONAL COMUM (COP)

É uma imagem no tempo que reflecte as notícias acerca de forças amigas (imagem azul), neutras (imagem verde ou branca), adversárias (imagem vermelha) e, do campo de batalha (imagem castanha). É formada através da base de dados das operações, das notícias e informações comuns a todos os escalões de comando e é disseminada ao seu escalão de comando.

INDICADORES

São definidos como manifestações, positivas ou negativas, da actividade inimiga ou qualquer aspecto específico da área de operações que podem revelar determinada vulnerabilidade do inimigo, indicar a adopção ou rejeição (pelo inimigo) de determinadas modalidades de acção ou influenciar a escolha (pelo comandante) de uma modalidade de acção. Também podem ser designados por indícios técnicos.

INDICADORES DE ALERTA E AVISO

São os indicadores relacionados com os preparativos de agressão por parte de um inimigo, alguns dos quais darão um aviso oportuno da iminência das hostilidades.

INDICADORES DE COMBATE OU TÁCTICOS

Estes indicadores revelam o tipo de operação que o inimigo está prestes a realizar. Cada tipo de operação vai obrigar a uma preparação específica e característica. Os indicadores ligados a estas preparações podem ser definidos antes das operações e ligados a tipos de operações específicas.

INDICADORES DE IDENTIFICAÇÃO

São os indicadores que permitem a identificação e acção de uma formação, unidade ou instalação, a partir do conhecimento da sua organização, equipamento e táctica.

INDÍCIOS TÉCNICOS

O mesmo que Indicadores.

INFORMAÇÃO/INFORMAÇÕES

Entende-se por informação ou informações (intelligence) o produto resultante do processamento de notícias respeitantes a nações estrangeiras, organizações ou elementos, reais ou potencialmente hostis, ou áreas de operações actuais ou potenciais. O termo também se aplica às actividades que visam obter o resultado final e bem assim às organizações empenhadas em tais actividades.

Entende-se, também, por informação os elementos que contribuem para o conhecimento do inimigo provável ou actual e da área de operações.

INFORMAÇÃO ACÚSTICA (ACINT)

É a informação obtida através da pesquisa e análise de fenómenos acústicos.

INFORMAÇÃO DE COMUNICAÇÕES (COMINT)

É a informação proveniente da interceptação por outros, que não os seus destinatários previstos, de comunicações rádio e sistemas de comunicações, bem como de características técnicas dessas transmissões.

INFORMAÇÃO ELECTRÓNICA (ELINT)

É a informação proveniente da interceptação por outros, que não os seus destinatários previstos, de emissões electromagnéticas (não-comunicações, p.e. ajudas à navegação e radares), que não são comunicações rádio, bem como das suas características técnicas.

INFORMAÇÃO DE FONTE ABERTA (OSINT)

É resultante da informação pública disponibilizada, bem como de outra não classificada cuja distribuição ou acesso público é restrito. É obtida em órgãos de comunicação social, designadamente imprensa escrita, televisão, rádio, internet, publicações técnicas e propaganda estatal.

INFORMAÇÃO HUMANA (HUMINT)

É a informação obtida de notícias fornecidas por origens humanas, ou seja, notícias recolhidas e fornecidas por pessoal treinado, junto de pessoas e meios multimédia para identificar elementos, intenções, composição, potencial, dispositivo, tácticas, equipamento, pessoal e capacidades inimigas.

INFORMAÇÃO DE IMAGENS (IMINT)

É a informação que tem por base imagens captadas por sensores – ópticos (do espectro visível), infravermelhos, radares e imagens multiespectrais – instalados em plataformas terrestres, navais, aéreas ou espaciais.

INFORMAÇÃO DE MEDIÇÃO E ASSINATURAS ELECTROMAGNÉTICAS (MASINT)

É informação científica e técnica obtida pela análise quantitativa e qualitativa dos dados (métricos, espaciais, comprimento de onda, dependência do tempo, modulação, plasma e hidromagnético, etc.), provenientes de objectos/alvos e fontes fixas ou dinâmicas, que contribui para a sua detecção, localização, seguimento, identificação e/ou descrição.

INFORMAÇÃO DE RADARES (RADINT)

É a informação obtida pela utilização de radares como principal meio de pesquisa e aquisição.

INFORMAÇÃO DE TRANSMISSÕES ELECTROMAGNÉTICAS E COMUNICAÇÕES (SIGINT)

A SIGINT é o termo geral para designar a Informação de Comunicações (COMINT) e a Informação Electrónica (ELINT), quando não se torne necessário fazer a distinção entre os dois tipos de informação, ou para englobar os dois termos.

INFORMAÇÕES, VIGILÂNCIA, AQUISIÇÃO DE OBJECTIVOS E RECONHECIMENTO (ISTAR)

Define-se como uma actividade de informações que integra e sincroniza o planeamento e a operação de sensores e equipamentos e os sistemas de processamento, exploração, targeting e disseminação, em apoio directo a operações correntes e futuras.

INFORMAÇÕES BÁSICAS

Informações básicas são as informações de fundo sobre um assunto, as quais são mantidas em bases de dados e continuamente actualizadas em tempo de paz e no decurso de operações.

INFORMAÇÕES BIOGRÁFICAS

São as informações sobre os pensamentos, hábitos, qualificações, aptidões, importância, relacionamento, estado de saúde e *curriculum vitae* sobre qualquer pessoa, com interesse actual ou potencial para as informações.

INFORMAÇÕES CORRENTES

Definem-se por informações relativas à situação corrente, quer a nível estratégico quer tático.

INFORMAÇÕES ECONÓMICAS

São as informações respeitantes a recursos económicos, actividades e políticas de entidades estrangeiras; incluindo a produção, distribuição e consumo de bens e serviços, emprego, finanças e outros aspectos do sistema económico internacional, tais como o comércio e investimento.

INFORMAÇÕES DE ENGENHARIA

São o produto do processamento da informação referente às operações de engenharia inimigas, recursos, condições ambientais, informação geográfica militar e terreno, necessárias ao comandante para o planeamento das operações de combate.

INFORMAÇÕES ESTRATÉGICAS

Informações estratégicas são informações necessárias à formulação de planos políticos e militares, a nível nacional e internacional. Este é o mais alto nível de informações, derivado das notícias recolhidas em resposta às necessidades colocadas pelos governos nacionais, cobrindo todo o espectro de assuntos militares, diplomáticos, políticos e económicos, nacional e internacional.

INFORMAÇÕES SOBRE FORÇAS ARMADAS

São as informações relativas a todos os aspectos das forças terrestres, navais, aéreas e espaciais inimigas ou potenciais, incluindo a ordem da batalha, comando e controlo, sistemas

de armas, treino, pessoal, doutrina, estratégia e táticas, logística, negócios de armamento, indústrias de defesa e despesas com a defesa.

INFORMAÇÕES GEOESPACIAIS

As informações geoespaciais consistem na exploração e análise das imagens de satélite, que visualizam, avaliam e descrevem os aspectos físicos e geográficos da área analisada.

INFORMAÇÕES SOBRE INFRA-ESTRUTURAS

São as informações respeitantes à rede ferroviária, estradal, de *pipelines*, de distribuição de água e sistemas de telecomunicações.

INFORMAÇÕES LOGÍSTICAS

São as informações respeitantes à capacidade de movimentar forças, apoiar e sustentar operações militares.

INFORMAÇÕES MÉDICAS

As informações médicas são as obtidas em resultado do processamento médico, bio-científico, epidemiológico, ambiental e outra informação relacionada com a saúde humana ou animal. Esta informação, sendo de natureza técnica específica, exige peritos da área de saúde durante as fases de orientação do esforço de pesquisa e processamento do ciclo da produção da informação.

INFORMAÇÕES DE OBJECTIVOS

Informações de objectivos definem-se por informações que retratam e localizam as componentes de um objectivo ou conjunto de objectivos e indicam as vulnerabilidades e importância relativa.

INFORMAÇÕES OPERACIONAIS

Informações operacionais são informações necessárias para o planeamento e conduta de campanhas ao nível operacional. Mais especificamente, são as informações necessárias para o planeamento, execução e apoio a campanhas e operações, por parte do Quartel-General Conjunto, no âmbito da Área de Operações Conjuntas (JOA). São informações que são produzidas no âmbito da Área de Interesse (AOI) do Comandante da Força Conjunta.

INFORMAÇÕES POLÍTICAS

São as informações a respeito da dinâmica dos casos políticos internos e externos de países estrangeiros, grupos regionais, acordos e tratados multilaterais, e movimentos políticos estrangeiros de apoio ou contestação a governos e autoridades estabelecidos. Inclui estruturas do governo, políticas internas e estrangeiras.

INFORMAÇÕES DE SEGURANÇA (SI)

São definidas como informações sobre a identidade, potencialidades e intenções de organizações hostis ou indivíduos que estão ou podem vir a estar envolvidos em actividades de espionagem, sabotagem, subversão ou terrorismo.

INFORMAÇÕES SOCIOLÓGICAS

São as informações respeitantes aos factores de ordem social e cultural, incluindo dados sobre a população, etnias, estratos e estabilidade social, opinião pública, instrução, religião, saúde, história, língua, valores, percepções e comportamento.

INFORMAÇÕES TÁCTICAS

Informações tácticas são as informações necessárias ao planeamento e conduta de operações tácticas. São informações usadas ao nível dos quartéis-generais das unidades de baixos escalões e são produzidas nas áreas destas unidades.

INFORMAÇÕES SOBRE TARGETING

São as informações que permitem enquadrar e localizar os componentes de um objectivo ou de um conjunto de objectivos; indicando a sua identificação, vulnerabilidades e importância relativa.

INFORMAÇÕES TÉCNICAS (TECHINT)

São as informações relativas a desenvolvimentos tecnológicos estrangeiros e das capacidades operacionais do equipamento estrangeiro que têm, ou podem vir a ter, uma aplicação prática para fins militares. São uma subdivisão das STI.

INFORMAÇÕES TÉCNICAS E CIENTÍFICAS (STI)

São as informações sobre as inovações verificadas no estrangeiro, no que diz respeito à investigação e desenvolvimento técnico e científico, incluindo técnicas de engenharia e de produção, novas tecnologias, sistemas de armas e suas capacidades.

INIMIGO

Refere-se a uma entidade, grupo ou força identificada como hostil às nossas forças e em que a aplicação da força está prevista. Existe declaração de guerra.

INTEGRAÇÃO

É um passo da fase de Processamento do Ciclo da Produção da Informação que consiste na combinação dos elementos individualizados, obtidos por análise, com outras notícias ou informações já conhecidas, a fim de se formularem uma ou mais hipóteses lógicas.

INTERPRETAÇÃO

É o passo final da fase de Processamento do Ciclo da Produção da Informação e consiste na determinação do significado de uma notícia relativamente a outras notícias ou informações já existentes. É onde a notícia registada, avaliada, analisada e integrada deve ser finalmente interpretada, para concluir o processo de conversão de notícia em informação.

INTERROGATÓRIO

Interrogatório é o esforço sistemático na procura de notícias que respondam às necessidades específicas de pesquisa, através de perguntas directas ou indirectas, a pessoas sob custódia das forças que o conduzem.

LINHAS DE DECISÃO (DL)

São linhas desfasadas no tempo e no espaço em relação às respectivas Áreas de Objectivos de Interesse, em que o comandante tem de tomar uma decisão para usar os seus meios, se quiser influenciar a operação numa determinada Áreas de Objectivos de Interesse.

MATRIZ DE SINCRONIZAÇÃO ISTAR

É uma representação gráfica que liga o Plano de Pesquisa às necessidades de informações do comandante.

NECESSIDADES DE INFORMAÇÃO (IR)

São definidas como aqueles itens de informação a respeito das características da área de operações e do inimigo que precisam de ser pesquisados e processados para responder às necessidades de informação do comandante. Também podem ser designados por quesitos concretos.

NECESSIDADES DE INFORMAÇÃO CRÍTICA DO COMANDANTE (CCIR)

Questões que dizem respeito ao estado de operacionalidade e capacidades de forças amigas, ao estado de operacionalidade, capacidades e intenções do inimigo e características da área de operações.

NECESSIDADES DE INFORMAÇÃO SOBRE FORÇAS AMIGAS (FFIR)

As FFIR consistem na informação que o comandante e o estado-maior precisam de saber acerca das nossas forças disponíveis para a operação. As FFIR garantem informação acerca da missão, unidades, tempo disponível, grau de operacionalidade e instrução; ou seja, como me visualizo.

NECESSIDADES PRIORITÁRIAS DE INFORMAÇÕES (PIR)

Consistem na informação mais importante que o comandante e o estado-maior necessitam de saber acerca do inimigo, quais as suas intenções, capacidades operacionais, incluindo o tempo disponível para o inimigo e o meio envolvente (terreno, condições meteorológicas e considerações civis); ou seja, como se visualiza o inimigo.

NOTÍCIA

Entende-se por notícia todo o dado não processado de qualquer natureza que pode ser usado na produção de informações.

OBJECTIVOS DE ELEVADO VALOR (HVT)

São objectivos (forças, meios e capacidades) que o comandante inimigo necessita para a condução bem sucedida de uma modalidade de acção específica.

OBJECTIVOS REMUNERADORES (HPT)

São objectivos cuja destruição ou neutralização contribui significativamente para o sucesso da operação amiga e para o fracasso da modalidade de acção do inimigo.

OPERAÇÕES DE CONTACTO

São operações táticas, abertas às actividades de pesquisa que incluam origens humanas para identificar atitudes, intenções, composição, potencial, dispositivo, táticas, equipamento, desenvolvimento de alvos, pessoal e capacidades dos elementos que sejam ou possam vir a ser potenciais ameaças às forças nacionais ou multinacionais.

OPERAÇÕES DE INFORMAÇÃO (INFO OPS)

Acções coordenadas que visam influenciar os decisores e o processo de decisão do inimigo ou terceiros, em apoio dos nossos objectivos políticos e militares, afectando os seus sistemas de Comando e Controlo e Informações (C2I) e os seus Sistemas de Informação e Comunicações (CIS), ao mesmo tempo que exploram/protegem os nossos sistemas C2I e CIS.

OPERAÇÕES CONJUNTAS

As operações conjuntas são definidas como operações nas quais podem estar envolvidos elementos de mais do que um ramo, podendo envolver forças aéreas, espaciais, navais, anfíbias, terrestres ou de operações especiais.

OPERAÇÕES PSICOLÓGICAS (PSYOPS)

As actividades psicológicas planeadas que utilizam meios de comunicação e outros meios, dirigidas sobre audiências aprovadas de forma a influenciar atitudes, a percepção e comportamentos que contribuam para a realização de objectivos políticos e militares.

OPONENTE

Refere-se a uma entidade, grupo ou força identificada que oferece resistência às nossas forças e em que a aplicação da força não está prevista. Não existe declaração de guerra.

ORDEM DE PESQUISA

Questões específicas colocadas a origens e órgãos de pesquisa orgânicos ou atribuídos.

ÓRGÃO DE PESQUISA

Um órgão de pesquisa é qualquer indivíduo, entidade ou unidade que obtém ou processa notícias. Por oposição, a origem pode ter a capacidade de pesquisar e processar ou simplesmente a de pesquisar, necessitando neste caso de a passar a outro órgão para a processar. A designação de órgãos de pesquisa engloba igualmente os órgãos que pesquisam notícias e aqueles que produzem informações.

ORIENTAÇÃO DO ESFORÇO DE PESQUISA

A que também se pode chamar direcção, é a primeira fase do Ciclo da Produção da Informação e consiste na determinação das necessidades de informações, no planeamento do esforço de pesquisa, na emissão de ordens e pedidos aos órgãos de pesquisa e na manutenção de uma contínua verificação da sua produtividade.

ORIGENS DE NOTÍCIAS

As origens de notícias são as fontes (pessoas, coisas ou acções) de que provêm todas as notícias pesquisadas acerca do inimigo e da área de operações. A origem é assim a fonte primária da informação e/ou possui ela mesmo a informação ou, ainda, pela sua actividade revela a existência de informação. Em contraponto, um sensor será então a pessoa ou sistema que obtém a notícia para a origem. Também podem ser designadas apenas por fontes.

PEDIDO DE PESQUISA (RFI)

Forma na qual uma necessidade de informação é comunicada às entidades de Gestão das Necessidades de Informações e Coordenação da Pesquisa, a escalões superiores, subordinados ou adjacentes.

PESQUISA

É a segunda fase do Ciclo da Produção da Informação e é definida como a exploração dos meios pelas origens e órgãos de pesquisa e a entrega da informação obtida à unidade de processamento apropriada para produção de informações. É o processo no qual as informações são pesquisadas para responder às necessidades de informações do comandante, identificadas na fase de orientação do esforço de pesquisa do Ciclo da Produção da Informação.

PONTOS DE DECISÃO (DP)

São pontos desfasados no tempo e no espaço em relação às respectivas Áreas de Objectivos de Interesse, em que o comandante tem de tomar uma decisão para usar os seus meios, se quiser influenciar a operação numa determinada Áreas de Objectivos de Interesse.

PLANO DE PESQUISA

Define-se como um plano para a recolha de notícias de todas as origens disponíveis, a fim de satisfazer as necessidades de informações e transformá-las em ordens e/ou pedidos aos órgãos de pesquisa apropriados. Trata-se de um documento de trabalho da célula de informações, que não constitui um apêndice ao anexo de informações e, como tal, não é difundido.

PROCESSAMENTO

O processamento é a parte do Ciclo da Produção da Informação em que as notícias que foram pesquisadas, em resposta à orientação do comandante, são convertidas em informações. É

definido como a transformação de notícias em informações através do registo, avaliação, análise, integração e interpretação.

PROTECÇÃO DA FORÇA (FP)

Abrange todas as medidas adoptadas e meios usados para minimizar a vulnerabilidade do pessoal, instalações, equipamento e operações a qualquer ameaça, em todas as situações, a fim de conservar a liberdade de acção e eficácia operacional de uma força.

QUESITOS CONCRETOS

O mesmo que Necessidade de Informação (IR).

RECONHECIMENTO

É definido, em termos ISTAR, como uma missão destinada a obter notícias, através da observação visual ou outros meios de detecção, relativas às actividades e recursos do inimigo, potencial ou não, bem como obter dados sobre as características meteorológicas, hidrográficas ou geográficas de uma determinada área.

REDUNDÂNCIA

Em termos de Informações, é um processo deliberado que utiliza mais de um meio para pesquisar o mesmo alvo.

REGISTO

É um passo na fase de Processamento do Ciclo da Produção da Informação, que consiste no agrupamento sistemático de todas as notícias, criando um registo de acontecimentos, de forma a facilitar a sua ulterior transformação em informações e a elaboração de documentos de informações.

RELATÓRIO IMEDIATO (RELIM)

É um relatório que contém notícias ou informações de valor tático imediato, para as quais a velocidade de transmissão é de importância fundamental. Em regra, dizem respeito a um só assunto.

RELATÓRIO DE INFORMAÇÕES (INTREP)

É um relatório difundido sem obediência a horários, sempre que as notícias ou informações disponíveis exigem a atenção do comandante destinatário. Este relatório deve conter algumas

PDE 2-00 Informações, Contra-Informação e Segurança

deduções derivadas das notícias e informações disponíveis na altura, as quais devem, em princípio, merecer a aprovação do comandante.

RELATÓRIO PERIÓDICO DE INFORMAÇÕES (PERINTREP)

Documento de disseminação que contém elementos de informação relativos à situação e actividades do inimigo, às suas possibilidades e vulnerabilidades, às características da área de operações e às acções de contra-informação, sob a forma de um resumo ordenado de notícias pesquisadas e processadas durante um período superior ao do Sumário de Informações.

RELATÓRIO SUPLEMENTAR DE INFORMAÇÕES (SUPINTREP)

Este relatório pode ser elaborado a pedido ou na previsão de certas operações. Destina-se a coligir informações sobre um ou mais assuntos específicos com vista à preparação de uma determinada operação ou a recapitular todas as informações obtidas durante um período de tempo prolongado.

SEGURANÇA

Em termos de Informações, a segurança é definida como a condição obtida quando a informação, o material, o pessoal, as actividades e as instalações estão protegidos contra a espionagem, a sabotagem, a subversão e o terrorismo, assim como contra perdas ou divulgações não autorizadas.

SEGURANÇA DAS OPERAÇÕES (OPSEC)

É o processo que confere a uma operação militar ou exercício a segurança apropriada, usando meios activos ou passivos, para negar ao inimigo o conhecimento dos dispositivos, capacidades e intenções das forças amigas.

SENSOR

Um sensor é a pessoa ou sistema que obtém notícia para a fonte.

SUBVERSÃO

A subversão é definida como uma acção designada para enfraquecer a força militar, económica ou política de uma nação pelo enfraquecimento da moral, da lealdade e da confiança dos seus cidadãos.

SUMÁRIO DE INFORMAÇÕES (INTSUM)

É um relatório de informações conciso que contém, além das mais recentes notícias cujo processamento ainda não foi possível, um resumo das principais informações obtidas durante o período a que diz respeito, sobre a situação do inimigo, suas actividades e possibilidades e características da área de operações.

TARGETING

Define-se como o processo de selecção de objectivos e determinação das respostas adequadas a efectuar nos mesmos, tendo em consideração os requisitos operacionais e as capacidades dos diversos sistemas.

TEMPO DE RELATO

É o intervalo de tempo entre a detecção de um item de informação por um sensor e a sua recepção por um analista.

TERRORISMO

O terrorismo pode ser definido como a utilização ilegal, de forma efectiva ou potencial, da força ou violência contra pessoas ou bens, tentando coagir ou intimidar governos ou sociedades, para alcançar objectivos políticos, religiosos ou ideológicos.

TRANSPARENTE ISTAR

É uma representação gráfica do Plano de Pesquisa.

VIGILÂNCIA

Define-se, em termos de ISTAR, como a observação sistemática do espaço aéreo, áreas superficiais ou sub-superficiais, lugares, pessoas ou coisas através de meios visuais, acústicos, electrónicos, fotográficos ou outros.

Página intencionalmente em branco

GLOSSÁRIO DE ABREVIATURAS

A

A2	<i>Air Intelligence Cell</i>	Célula de Informações Aéreas
ACINT	<i>Acoustic Intelligence</i>	Informação Acústica
ACO	<i>Allied Command for Operations</i>	Comando Aliado para as Operações
ADP	<i>Automatic Data Processing</i>	Processamento Automático de Dados
AGM	<i>Attack Guidance Matrix</i>	Matriz Guia de Ataque
AOI	<i>Area of Interest</i>	Área de Interesse
AIR	<i>Area of Intelligence Responsibility</i>	Área de Responsabilidade de Informações
AIRINTREP	<i>Air Intelligence Report</i>	Relatório de Informações Aéreas
AIS	<i>Automated Information System</i>	Sistema Automático de Informação
AJF	<i>Allied Joint Force</i>	Força Conjunta da Aliança
AJP	<i>Allied Joint Publication</i>	
AOO	<i>Area of Operations</i>	Área de Operações
ASAS	<i>All Source Analysis System</i>	
ASC	<i>All Source Cell</i>	Célula de Todas as Origens
ASTOR	<i>Airborne Stand Off Radar</i>	Aeronave com um sistema de radar

B

BDA	<i>Battle Damage Assessment</i>	Avaliação dos Danos no Espaço de Batalha
BICC	<i>BICES Initial Core Capability</i>	
BICES	<i>Battlefield Information Collection and Exploitation Systems</i>	

C

C2	<i>Command and Control</i>	Comando e Controlo
C4I		Comando, Controlo, Comunicações, Computadores e Informações
CBRN	<i>Chemical, Biological, Radiological and Nuclear</i>	Nuclear, Biológica, Química e Radiológica (NBQR)
CC	<i>Collection Coordination</i>	Coordenação da Pesquisa
CCIR	<i>Commander's Critical Information Requirements</i>	Necessidades de Informação Crítica do Comandante
CCIRM	<i>Collection Coordination and Intelligence Requirements Management</i>	Gestão das Necessidades de Informações e Coordenação da Pesquisa
CENTRIXS	<i>Combined Enterprise Regional Information Exchange System</i>	
CHOD	<i>Chief of Defence</i>	Chefe do Estado-Maior General das Forças Armadas
CI	<i>Counter-Intelligence</i>	Contra-Informação
CIMIC	<i>Civil-military Co-operation</i>	Cooperação Civil Militar
CIS	<i>Communications and Information System</i>	Sistema de Informação e Comunicações
CJTF	<i>Combined Joint Task Force</i>	Força Tarefa Conjunta Combinada
CJTFFHQ	<i>Combined Joint Task Force Headquarters</i>	Quartel-General da Força Tarefa Conjunta Combinada
CM		Corredor de Mobilidade
CoA	<i>Course of Action</i>	Modalidade de Acção (m/a)
CoG	<i>Centre of Gravity</i>	Centro de Gravidade

NÃO CLASSIFICADO

PDE 2-00 Informações, Contra-Informação e Segurança

COMCJTF	<i>Commander of Combined Joint Task Force</i>	Comandante da Força Tarefa Conjunta Combinada
COMINT	<i>Communications Intelligence</i>	Informação de Comunicações
CONOPS	<i>Concept of Operations</i>	Conceito de Operação
COP	<i>Common Operational Picture</i>	Imagem Operacional Comum
CPG	<i>Commander's Planning Guidance</i>	Directiva de Planeamento do Comandante
CRO	<i>Crisis Response Operations</i>	Operações de Resposta a Crises
CRONOS	<i>Crisis Response Operations in NATO Open System(s)</i>	
CT	<i>Counter Terrorism</i>	Contra-Terrorismo
D		
DJTF	<i>Deployable Joint Task Force</i>	Força Tarefa Conjunta Projectável
DL	<i>Decision Line</i>	Linha de Decisão
DOCEX	<i>Document Exploitation</i>	Exploração de Documentos
DP	<i>Decision Point</i>	Ponto de Decisão
E		
EApprox		Eixo de Aproximação
EEFI	<i>Essential Elements of Friendly Information</i>	Elementos Essenciais de Informação das Forças Amigas
ELINT	Electronic Intelligence	Informação Electrónica
EM		Estado-Maior
ESM	<i>Electronic Support Measures</i>	Medidas de Apoio Electrónico
EW	<i>Electronic Warfare</i>	Guerra Electrónica
F		
FFIR	<i>Friendly Forces Information Requirements</i>	Necessidades de Informação sobre Forças Amigas
FP	<i>Force Protection</i>	Protecção da Força
G		
G2	<i>Ground Intelligence Cell</i>	Célula de Informações Terrestres
GIS	<i>Geographic Information System</i>	Sistema de Informação Geográfica (SIG)
H		
HIS	<i>Hostile Intelligence Services</i>	Serviços de Informações Hostis
HN	Host Nation	Nação Hospedeira
HNS	Host Nation Support	Apoio da Nação Hospedeira
HPT	<i>High-Payoff Target</i>	Objectivo Remunerador
HPTL	High-Payoff Targets List	Lista de Objectivos Remuneradores
HQ	<i>Headquarters</i>	Quartel-General (QG)
HUMINT	<i>Human Intelligence</i>	Informação Humana
HVT	<i>High Value Target</i>	Objectivo de Elevado Valor
HVTL	<i>High Value Targets List</i>	Lista de Objectivos de Elevado Valor
I		
I&W	<i>Indications and Warning</i>	Indicações e Avisos
IE	<i>Intelligence Estimate</i>	Estudo da Situação de Informações
IFS	<i>Intelligence Functional Service</i>	Serviços Funcionais de Informações

IMINT	Imagery Intelligence	Imagens de Informação
IMP	<i>Intelligence Management Plan</i>	Plano de Gestão das Informações
INFO OPS	<i>Information Operations</i>	Operações de Informação
INFOSEC	<i>Information Security</i>	Segurança da Informação
INTREP	<i>Intelligence Report</i>	Relatório de Informações
INTSUM	<i>Intelligence Summary</i>	Sumário de Informações
IO	International Organisations	Organizações Internacionais (OI)
IPB	<i>Intelligence Preparation of Battlefield</i>	Estudo do Espaço de Batalha pelas Informações
IR	<i>Information Requirements</i>	Necessidades de Informação
IRM	<i>Intelligence Requirements Management</i>	Gestão das Necessidades de Informações
ISTAR	<i>Intelligence, Surveillance, Target Acquisition and Reconnaissance</i>	Informações, Vigilância, Aquisição de Objectivos e Reconhecimento
IUSS	<i>Integrated Underwater Surveillance System</i>	Sistemas Integrados de Vigilância Subaquática

J

JFC	<i>Joint Force Commander</i>	Comandante da Força Conjunta
JHQ	<i>Joint Headquarters</i>	Quartel-General Conjunto
JIC	<i>Joint Intelligence Centre</i>	Centro de Informações Conjunto
JIOCC	<i>Joint INFO OPS Coordination Cell</i>	Célula de Coordenação de INFO OPS Conjuntas
JIPB	<i>Joint Intelligence Preparation of the Battlespace</i>	Estudo Conjunto do Espaço de Batalha pelas Informações
JIPTL	<i>Joint Integrated Prioritised Target List</i>	Lista de Objectivos Conjunta, Integrada e Priorizada
JITL	<i>Joint Integrated Target List</i>	Lista de Objectivos Conjunta e Integrada
JOA	<i>Joint Operational Area</i>	Área de Operações Conjuntas
JOIIS	<i>Joint Operations Intelligence Information System</i>	
JTF	<i>Joint Task Force</i>	Força Tarefa Conjunta
JTL	<i>Joint Target List</i>	Lista de Objectivos Conjunta
JTS	<i>Joint Targeting System</i>	Sistema Conjunto de <i>Targeting</i>

L

LAN	<i>Local Area Network</i>	Redes de Área Local
LANDINTREP	<i>Land Intelligence Report</i>	Relatório de Informações Terrestres
LO	<i>Liaison Officier</i>	Oficial de Ligação
LOCE	<i>Linked Operations-Intelligence Centres Europe</i>	
LTIOV	<i>Latest Time Information Of Value</i>	Tempo de Validade da Informação

M

m/a	<i>Course of Action (CoA)</i>	Modalidade de Acção
MARINTREP	<i>Maritime Intelligence Report</i>	Relatório de Informações Navais
MASINT	<i>Measurement and Signatures Intelligence</i>	Informação de Medição e Assinaturas Electromagnéticas
MC	Mobility Corridor	Corredor de Mobilidade
ME	<i>Main Effort</i>	Esforço
MJO	<i>Major Joint Operations</i>	Operações Conjuntas de Grande Envergadura

NÃO CLASSIFICADO

PDE 2-00 Informações, Contra-Informação e Segurança

MOD	<i>Ministry of Defence</i>	Ministério da Defesa
MOOTW	<i>Military Operations Other Than War</i>	Outras Operações Militares Que Não-Guerra
MoU	<i>Memorandum of Understanding</i>	Memorando de Entendimento
N		
N2	<i>Navy Intelligence Cell</i>	Célula de Informações Navais
NAI	<i>Named Area of Interest</i>	Área Designada de Interesse
NATO	<i>Wide Area Network</i>	Rede OTAN Secreta
SECRET		
WAN		
NBA	<i>NATO BICES Agency</i>	
NBQR	<i>Nuclear, Biological, Chemical and Radiological (CBRN)</i>	Nuclear, Biológica, Química e Radiológica
NCIA	<i>National Counter-Intelligence Adviser</i>	Conselheiro Nacional para Assuntos de Contra-Informação
NCIR	<i>National Counter-Intelligence Representatives</i>	Representantes Nacionais para Assuntos de Contra-Informação
NCS	<i>NATO Command Structure</i>	Estrutura de Comandos da OTAN
NEP	<i>Standing Operating Procedures (SOP)</i>	Normas de Execução Permanente
NEO	<i>Noncombatant Evacuation Operations</i>	Operações de Evacuação de Não-Combatentes
NGO	<i>Non-Governmental Organisation</i>	Organizações Não-Governamentais (ONG)
NIC	<i>National Intelligence Cells</i>	Células Nacionais de Informações
NNTCN	<i>Non-NATO Troop Contributing Nations</i>	Nações Contribuintes Não OTAN
NSTL	<i>No-Strike Target List</i>	Lista de Objectivos a Não Atacar
NWIA	<i>NATO-Wide Intelligence Architectures</i>	Arquitectura das Informações na OTAN
O		
OI	<i>International Organisations (IO)</i>	Organizações Internacionais
ONG	<i>Non-Governmental Organisation (NGO)</i>	Organizações Não-Governamentais
OPCOM	<i>Operational Command</i>	Comando Operacional
OPCON	<i>Operational Control</i>	Controlo Operacional
OPG	<i>Operations Planning Group</i>	Grupo de Planeamento das Operações
OPLAN	<i>Operational Plans</i>	Planos de Operações
OPP	<i>Operational Planning Process</i>	Processo de Planeamento Operacional
OPSEC	<i>Operations Security</i>	Segurança das Operações
ORBAT	<i>Order of Battle</i>	Ordem de Batalha
OSINT	<i>Open Source Intelligence</i>	Informação de Fonte Aberta
P		
PDM		Processo de Decisão Militar
PE	<i>Peace Enforcement</i>	Imposição de Paz
PERINTREP	<i>Periodic Intelligence Report</i>	Relatório Periódico de Informações
PI	<i>Public Information</i>	Informação Pública
PIR	<i>Priority Intelligence Requirements</i>	Necessidades Prioritárias de Informações
PK	<i>Peacekeeping</i>	Manutenção de Paz
PL	<i>Phase Line</i>	Linha de Fase
PRC		Potencial Relativo de Combate
PSO	<i>Peace Support Operations</i>	Operações de Apoio à Paz
PSYOPS	<i>Psychological Operations</i>	Operações Psicológicas

Q

QG	<i>Headquarters (HQ)</i>	Quartel-General
-----------	--------------------------	-----------------

R

RADINT	<i>Radar Intelligence</i>	Informação de Radares
RELIM		Relatório Imediato
RFI	<i>Request for Information</i>	Pedido de Pesquisa
RFIMS	<i>Request for Information Management System</i>	
RTL	<i>Restricted Target List</i>	Lista de Objectivos Restritos

S

SA	<i>Situational Awareness</i>	Avaliação da Situação
SAR	<i>Search and Rescue</i>	Busca e Salvamento
SC	<i>Strategic Commands</i>	Comandos Estratégicos
SHAPE	<i>Supreme Headquarters Allied Powers Europe</i>	
SI	<i>Security Intelligence</i>	Informações de Segurança
SIG	<i>Geographic Information System (GIS)</i>	Sistema de Informação Geográfica
SIGINT	<i>Signals Intelligence</i>	Informação de Transmissões Electromagnéticas e Comunicações
SIR	<i>Security Intelligence Requirements</i>	Necessidades de Informações de Segurança
SOP	<i>Standing Operating Procedures</i>	Normas de Execução Permanente (NEP)
SOR	<i>Statement of Requirements</i>	
STANAG	<i>Standardisation Agreement</i>	
STI	<i>Scientific and Technical Intelligence</i>	Informações Técnicas e Científicas
SUPINTREP	<i>Supplementary Intelligence Report</i>	Relatório Suplementar de Informações
SUPPLAN	<i>Support Plans</i>	Planos de Apoio

T

TACOM	<i>Tactical Command</i>	Comando Tático
TACON	<i>Tactical Control</i>	Controlo Tático
TAI	<i>Target Area of Interest</i>	Área de Objectivo de Interesse
TECHINT	<i>Technical Intelligence</i>	Informações Técnicas
TO		Teatro de Operações
TOC		Transparente de Obstáculos Combinados
TOC-M		Transparente de Obstáculos Combinados Modificado
TSCM	<i>Technical Surveillance Counter-Measures</i>	Contra-Medidas Técnicas de Vigilância
TTP	<i>Tactics, Techniques and Procedures</i>	Táticas, Técnicas e Procedimentos

U

UAV	<i>Unmanned Aerial Vehicle</i>	Aeronave Não-Tripulada
UE		União Europeia

V

VTC	<i>Video Teleconferencing</i>	Videoconferência
------------	-------------------------------	------------------

Página intencionalmente em branco

