BOLETIM INFORMATIVO DA ESCOLA PRÁTICA DE TRANSMISSÕES

mensagem

Março 2012



EID

Soluções para comunicações tácticas



Comunicações HF
por efeito NVIS



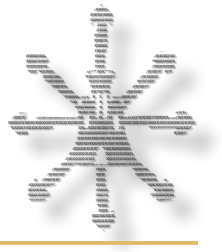
Rádios e
Sistemas de Intercomunicação



Ligação sem fios para Rádios e
Sistemas de Intercomunicação

shaping the future
... in DEFENCE COMMUNICATIONS

www.eid.pt



Ficha Técnica

Edição/Propriedade

Escola Prática Transmissões

Director

Cor Tm Rui Pinto

Direcção Técnica

Maj Tm (Eng) João Correia

Edição gráfica & design

Maj Tm João Correia
Alf Tm Nelson Amaral
Asp Tm João Teixeira

Capa

Alf Tm Nelson Amaral

Sumário

Editorial	4
Mensagem Director Honorário da Arma	6
O Sargento-Mor Adjunto do Comandante	7 a 14
Entrevista MGen Pinto de Castro	15 a 19
Superioridade de Informação no Exército . Um objetivo estratégico	20 a 36
Gestão da Informação no Exército	37 a 45
Gestão da Informação / Gestão da Informação - Uma Solução de Software	46 a 56
Novo conceito de Centro de Comunicações	57 a 69
"Desconflituar" – A Estrutura ISTAR e a Guerra Eletrónica	70 a 77
Guerra Eletrónica: Evolução de Conceitos na NATO	78 a 83
Sistema de Radiolocalização de Emissões Eletromagnéticas (SRE2)	84 a 91
Colaboração da EPT com as Autoridades e Entidades Civis e Militares	92 a 94
A certificação como valorização da carreira técnica do Sargento de Transmissões	95 a 100
Desenvolvimento de Sistemas de Informação para a defesa e segurança	101 a 111
Projecto, Realização e Estudo de um Agregado de Fendas	112 a116
Estudo das perturbações dos geradores eólicos na radiação das estações de suporte à navegação aérea	117 a 121
Signal Captains Career Course	122 a 126
Arma de Transmissões - Alguma estatística do ano de 2011	127 a 129
Jornadas Técnicas da Arma de Transmissões	130 a 132

Rohde & Schwarz - na vanguarda da tecnologia



Temos as melhores soluções para si.

A Rohde & Schwarz é um fabricante independente e um dos maiores fornecedores de equipamentos e sistemas electrónicos da Europa. Desenvolvemos, produzimos e comercializamos instrumentos e sistemas nas áreas de teste e medida, radiocomunicações, broadcasting, radiomonitorização e radiolocalização, segurança IT.

A chave do nosso sucesso é o desenvolvimento de sistemas de comunicação e medida em parceria com os nossos clientes. Esforçamo-nos para entender ao pormenor as necessidades dos nossos clientes, e depois desenhar soluções rentáveis. Como empresa independente, mantemos um contacto próximo com os nossos clientes através de uma rede de mais de 70 representações mundiais.

O nome Rohde & Schwarz é sinónimo de inovação, precisão, fiabilidade e qualidade. Esta é a nossa fórmula para atingirmos a satisfação do cliente e para sermos os melhores na nossa área de negócios.

www.rohde-schwarz.pt

ROHDE&SCHWARZ

Editorial

Saúdo todos aqueles que no último ano, com determinação, competência e entusiasmo cumpriram com êxito as mais diversas missões, confirmando o prestígio e a credibilidade da Casa-Mãe das Transmissões. Aproximam-se as Comemorações do Dia da Arma de Transmissões e da sua Escola, associando-se a esta data a realização das Jornadas Técnicas de Transmissões e a publicação de mais um número da revista Mensagem, que no seu conjunto constituem-se como um factor multiplicador de conhecimentos e experiências, que reforçam o espírito de corpo e a cultura característica da Arma de Transmissões.



Cor Tm Rui Pinto

A diversidade e densidade dos temas tratados neste número espelham de forma clara a complexidade das actividades desenvolvidas, não só pelos militares da EPT, mas também por aqueles que com eles colaboram e estão presentes em outras Unidades de TM. A constante evolução dos sistemas de comunicações e de informação são um desafio constante para aqueles que tem a responsabilidade de os desenvolver, implementar, manter e operacionalizar. Neste sentido a formação dos quadros de TM tem que ser permanentemente revista, actualizada e consolidada de forma a ser adequada às necessidades da operacionalização dos seus sistemas. A publicação desta revista pretende reflectir a excelência desta realidade.

A EPT, unidade especializada na área das tecnologias e sistemas de informação, continuará a afirmar-se pela qualidade, racionalidade e inovação, no desenvolvimento das suas actividades de formação, operacionais e de investigação e desenvolvimento, sempre alinhados com as orientações do Exército.

Certos que só com a conjugação dos conhecimentos e da vontade de todos conseguiremos ultrapassar os desafios que se avizinham, continuaremos a caminhar rumo ao futuro com convicção, responsabilidade, confiança e otimismo, servindo a Arma de Transmissões e o Exército, onde nos revemos no seu passado e em cujos valores continuaremos a acreditar.

O Comandante da EPT

Rui Manuel Nunes Pinto

Coronel Tm

O mundo é complexo.
As suas decisões não têm que ser.



As decisões no domínio da defesa são cada vez mais complexas. Na Thales servimos todos os ramos das forças armadas nas vertentes aérea, naval, terrestre, espacial e das operações conjuntas, abrangendo também as novas ameaças em ambientes de segurança urbana e no ciberespaço. A escalabilidade e interoperabilidade das nossas soluções e serviços proporcionam apoio operacional às missões onde o tempo e a fiabilidade são cruciais. Integrando todos os nossos sistemas, equipamentos e soluções na Cadeia de Decisão Crítica, permitimos aos decisores controlarem a complexidade em cenários críticos e tomarem decisões atempadas que permitem obter os melhores resultados.

Para saber mais sobre as nossas soluções para Defesa, procure o código QR ou visite o site em **thalesgroup.com**

THALES

Together • Smarter • Safer

Mensagem do Director Honorário da Arma



Tenente-General Quesada Pastor

É sempre com grande alegria que o Director Honorário da Arma de Transmissões se dirige neste dia festivo à sua Arma, através da Revista Mensagem.
Quando falo na nossa Arma refiro-me sobretudo às pessoas, homens e mulheres, que como praças, sargentos, oficiais e funcionários civis servem o Exército na Arma de Transmissões.
Quero também, juntamente com as pessoas, referir o conjunto de tradições, procedimentos e memórias que consubstanciam os valores que sedimentam a coesão da Arma, aquilo que na linguagem militar se chama, e bem, o espírito de corpo.

Com a mesma alegria me dirijo ao nosso Patrono São Gabriel, na certeza que a nossa mensagem, não tendo a certamente a mesma transcendência, se aproximará minimamente da sua eficácia.
O ano que passou, há que dizê-lo, não nos deixou demasiados motivos de alegria. A situação do país à qual as Forças Armadas, o Exército e a Arma de Transmissões não podem ser alheios nem indiferentes, trouxe-nos problemas ao nível do pessoal, da organização. Sentimos dificuldades que nos deixaram a todos, e em todos os escalões, perplexos e preocupados.
Também, neste ano que passou, deixaram o nosso convívio camaradas que a morte prematuramente levou. Permitam-me uma referência particular, pela amizade que nos uniu ao longo de tantos anos e pelo que ele foi para a Arma de Transmissões, ao Coronel Joaquim Stone. A forma apaixonada como viveu a sua vida e a sua dedicação à Arma de Transmissões são motivos mais do que suficientes para o evocar neste momento.
Mas se para a morte não há remédio, para além de honrar a sua memória, para as dificuldades que temos há algo a fazer. Nas palavras que o Presidente do Conselho da Arma de Transmissões me transmitiu, registei uma: “não baixamos os braços”.
É esta a ideia chave que vos quero deixar. Com inteligência, imaginação, conhecimento e bom senso teremos certamente a capacidade, de não baixando os braços, continuarmos a cumprir a missão.
Quero-vos ainda lembrar que as dificuldades e problemas que enfrentamos são certamente efémeros enquanto a nossa determinação é constante.
É por tudo isto que considero que “com engenho e ciência” e “sempre melhor” contando com todos vós será possível continuar a cumprir este desígnio da nossa Arma de Transmissões.

O Sargento-Mor Adjunto do Comandante



SMor Sabino Ferreira

Introdução

Já são mais de vinte os anos de permanência na Escola Prática de Transmissões, cuja contagem começou em 1983 com o início do 2º ano do 11º Curso de Formação de Sargentos e se prolongou até agora, sempre como minha primeira preferência e como "Porto seguro" no regresso das colocações fora da Guarnição Militar de Preferência (GMP).

Tanto tempo fez com que, para além de uma relação meramente profissional, tenha crescido aquela ligação afetiva que nos une às coisas e às pessoas que nos rodeiam durante o nosso crescimento como profissionais e como Homens.

Era com certeza essa afinidade que me impelia a, depois da promoção ao posto de Sargento-mor, ter como principal aspiração o desempenho das funções de adjunto do comandante[1] da minha Escola, pelo que foi com muita satisfação, uma enorme honra e grande orgulho, que aceitei o convite que me foi endereçado em 2007, pelo então Coronel Tm Arnauld Moreira e posteriormente renovado pelos Coronéis Tm, Pedro Melo e Rui Pinto, para o preenchimento deste cargo, que me tem permitido continuar a dar a minha contribuição para o cumprimento da missão da minha unidade[2].

Após um período de quase cinco anos no desempenho destas funções e porque há sempre aspetos que podem ser corrigidos e melhorados, sinto ser meu dever aproveitar esta experiência, que reflete, não só a minha vivência pessoal, mas também os inúmeros contactos e troca de impressões com os pares e militares das mais diversas unidades, para deixar um registo que possa servir de contributo para tornar as funções de adjunto do comandante mais estimulantes e motivadoras, e mais úteis à ação de comando.

Após um período de quase cinco anos no desempenho destas funções e porque há sempre aspetos que podem ser corrigidos e melhorados, sinto ser meu dever aproveitar esta experiência, que reflete, não só a minha vivência pessoal, mas também os inúmeros contactos e troca de impressões com os pares e militares das mais diversas unidades, para deixar um registo que possa servir de contributo para tornar as funções de adjunto do comandante mais estimulantes e motivadoras, e mais úteis à ação de comando.

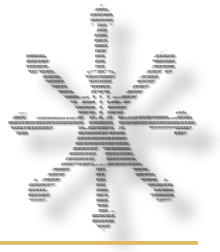
Para desenvolver o tema presente, para além da experiência profissional, procurei obter informação sobre o cargo equivalente nos exércitos dos países aliados, acabando por salientar, fundamentalmente, a doutrina do exército dos Estados Unidos da América (EUA), por ser a que, tradicionalmente, mais tem influenciado a nossa organização, nomeadamente na criação do próprio cargo de adjunto do comandante, ser a mais experimentada em cenários reais e por isso alicerçada em várias lições aprendidas. E também a do exército de Espanha pela proximidade geográfica e cultural.

Resenha Histórica do Cargo de Adjunto do Comando/Comandante

A criação do posto de Sargento-mor, juntamente com o de Sargento-chefe aliás, dá-se apenas em 1976 (decreto-lei 891/76 de 30 de Dezembro), sendo, assim, um acontecimento suficientemente recente para ser contemporâneo com alguns dos militares ainda presentes nas fileiras.

1 Sempre que a palavra "comandante" apareça no texto com sentido indefinido deverá ser entendido como Cmdt/Dir/Ch

2 Sempre que a palavra "unidade" apareça no texto com sentido indefinido deverá ser entendido como UU/EE/OO



Com este passo, dado com carácter de urgência segundo o texto do próprio decreto-lei, a categoria de sargentos passou a ter a estrutura hierárquica ainda hoje em vigor, ficando mais próxima da configuração dominante das categorias de sargentos das Forças Armadas dos países aliados.

Nesta sequência, surge naturalmente a necessidade da definição das respetivas funções, que foi suprida logo no dia seguinte através do decreto-lei 920/76 de 31 de Dezembro que, aliás, implementa uma grande reestruturação da categoria de sargentos do Quadro Permanente (QP) do Exército, podendo considerar-se, na parte correspondente, o embrião do Estatuto dos Militares das Forças Armadas (EMFAR), necessidade que o próprio decreto-lei reconhece, nos capítulos: hierarquia e funções; quadros; promoções; tirocínios estágios e cursos; e que, sobre as funções atribuídas ao sargento-mor, estabelece o seguinte: "Elemento do estado-maior do comando de unidades independentes de escalão batalhão, regimento e outras acima de batalhão ou equivalente, como adjunto do comandante para os assuntos relacionados com a vida interna da unidade, nomeadamente no que respeita à administração do pessoal e aos aspetos administrativo-logísticos e ainda, no Estado-maior do Exército, nos Quartéis-generais e Direções das Armas e Serviços."

Se em termos genéricos e estatutariamente estas são, ainda hoje, as funções atribuídas aos sargentos-mores adjuntos dos comandantes, organicamente e apesar do curto tempo de existência do posto e do cargo, sofreram uma significativa transformação.

Na primeira revisão da II parte (Serviço interno das unidades e de guarnição), do Regulamento Geral do Serviço do Exército (RGSE - Decreto de 6 de Junho de 1914), aprovada pelo Decreto n.º 49/80 de 22 de Julho que, a título de curiosidade, foi posta em execução, com carácter experimental, no Regimento de Infantaria de Beja, no Regimento de Artilharia de Leiria e no Regimento de Cavalaria de Braga, e posta em execução a título definitivo em todas as unidades e estabelecimentos militares do Exército a partir de 1 de janeiro de 1981 (Decreto-Lei 518/80 de 5 de novembro), são estipulados os deveres e atribuições inerentes às funções de serviço interno, do adjunto do comando de regimento (art.º 10º). Notando-se a alteração da designação do cargo em relação ao decreto-lei que o criou, de adjunto do comandante para adjunto do comando, são consagradas, entre outras atribuições, as seguintes:

1. O adjunto do comando do regimento ou unidade equivalente está na dependência direta do 2º comandante, a quem coadjuva no âmbito das atividades gerais do serviço interno durante o período de expediente normal.

2. Além dos deveres previstos neste e noutros regulamentos, compete-lhe:

   a. Ao iniciar o serviço, receber do ofi cial de dia o respetivo relatório, tomar con hecimento das ocorrências que exigem co ordenação de acionamento e obter para elas orientação superior, se necessário, e providenciar pela sua entrega na secretaria de comando

   b. Superintender, durante o período de expediente normal, nos serviços or dinário e eventuais interiores e vigiar a sua regular execução;

   c. Fazer executar às horas determi na das os toques indicados no horário de serviço;

   d. Presidir às formaturas da unidade que não sejam comandadas por qualquer oficial;

   e. Assistir às refeições das praças;

   f. Coordenar as atividades gerais da limpeza e conservação do aquartela mento;

g. Controlar a entrada e saída de forças, de acordo com as instruções do co mando;

h. Fiscalizar o serviço da guarda de polícia e o controle da entrada de estranhos no quartel;

i. Verificar o cumprimento das medi das contra incêndios e a proficiência do res petivo material;

j. Visitar diariamente os presos, ouvir as suas pretensões e dar delas conhecimen to superior, sem contender com a trami tação processual;

k. Zelar permanentemente quer pelo aprumo do pessoal, quer no que se refere ao cumprimento das determinações do co mandante e dos regulamentos, fazendo as propostas que entender convenientes no sentido de prevenir ou remediar qualquer desvio.

l. Nos dias de atividade normal, or ganizar a parada da guarda e apresentar a respetiva formatura ao oficial de dia.

A 3 de fevereiro de 1986, por despacho do Chefe do Estado-Maior do Exército, general Salazar Braga, é aprovado o Regulamento Geral do Serviço das Unidades do Exército (RGSUE), que entra imediatamente em vigor, em substituição do RGSE de 1914 e da II Parte do RGSE de 1980.

Neste regulamento, no seu art.º 11º da I parte, ficam determinados os seguintes deveres e atribuições inerentes às funções de serviço interno, para o sargento-mor adjunto do comando do regimento:

1. O sargento-mor é um elemento do comando do regimento e desempenha as funções de adjunto do comando para os assuntos relacionados com a vida interna da unidade, nomeadamente no que respeita à administração do pessoal e aos aspetos administrativo-logísticos.

2. Além dos deveres previstos neste e noutros regulamentos, compete-lhe:

a. Atuar, em nome do comandante, nos assuntos que digam diretamente res peito à classe de sargentos e servir de elo de ligação entre estes e o comandante;

b. Auxiliar, quando necessário, o esta do-maior da unidade nos assuntos rela tivos à administração do pessoal;

c. Zelar pelo atavio, apresentação, conduta e disciplina dos sargentos e praças, de acor do com as instruções do comandante;

d. Ministrar instrução aos sargentos de acordo com as suas aptidões e progra mas aprovados;

e. Acompanhar a vida interna da uni dade (exceto nos aspetos de serviço diário e segurança) no sentido da manutenção, em alto grau, da eficiência e da disciplina;

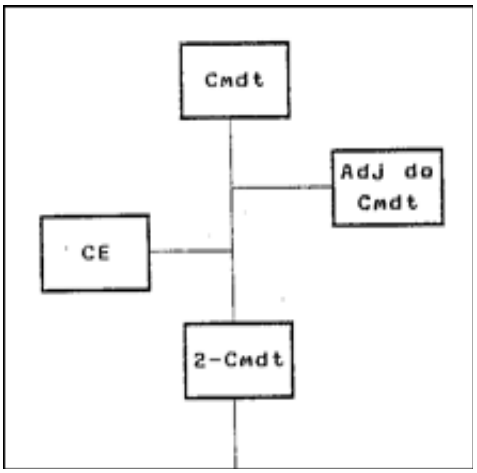
f. Nos dias de atividade plena, organi zar a parada da guarda e apresentar a res petiva formatura ao oficial de dia.

Passados aproximadamente quatro anos, é publicada a primeira versão do Estatuto dos Militares das Forças Armadas (EMFAR), decreto-lei 34A/90 de 24 de Janeiro, que manteve a essência do RGSUE e recupera a designação do cargo atribuída aquando da sua criação, como “adjunto do comandante de unidade independente de escalão batalhão ou superior…”.

Esta alteração passa a refletir-se nos Quadros Orgânicos de Pessoal (QOP) das unidades tipo Regimento, publicados em 1993, em cujo organigrama o sargento-mor aparece imediatamente a seguir e lateralmente ao comandante, como seu elemento

de apoio direto. Simultaneamente, nos mesmos QOP, o sargento-mor adjunto do comandante é colocado como sargento (chefe) de secretaria, criando uma situação indesejável de dupla dependência, do comandante da unidade e do chefe da secção de pessoal, uma vez que a secretaria da unidade estava, então, integrada na secção de pessoal.

Com a revisão dos QOP de 2006, esta última situação é alterada, o sargento-mor deixa de ser sargento (chefe) de secretaria e são criados os cargos de adjunto dos comandantes dos órgãos centrais de administração e direção (OCAD) e dos diretores das respetivas direções, replicando, quase fielmente, a distribuição dos sargentos-mores adjuntos de comandante na organização do exército dos EUA.



Recorte do organigrama da EPT dos QOP de 1993

É esta a distribuição dos cargos atualmente existente, cuja designação "adjunto do comandante" é consolidada com a alteração do EMFAR (decreto-lei n.º 236/99 de 25 de Junho) no seu art.º 273º, e a revisão da I parte do RGSUE (despacho de 14 de setembro de 2005 do general CEME), art.º 11º, e que define os seguintes deveres e atribuições inerentes às funções de serviço interno, ainda hoje atuais:

1. O sargento-mor é um elemento do comando do regimento ou do batalhão independente e desempenha as funções de adjunto do comandante para os assuntos relacionados com a vida interna da unidade, nomeadamente no que respeita à administração do pessoal, à formação dos sargentos e aos aspetos administrativos e logísticos; pode exercer funções de instrutor.

2. Além dos deveres previstos neste e noutros regulamentos, compete-lhe:

a. Atuar, em nome do comandante, nos assuntos que digam diretamente respeito à categoria de sargentos e servir de elo de ligação entre estes e o comandante;

b. Auxiliar, quando necessário, o estado-maior da unidade nos assuntos relativos à administração do pessoal;

c. Zelar pelo atavio, apresentação, conduta e disciplina dos sargentos e praças, de acordo com as instruções do comandante;

d. Acompanhar a vida interna da unidade (exceto nos aspetos de serviço diário e segurança) no sentido da manutenção, em alto grau, da eficiência e da disciplina;

e. Nos dias de atividade normal, organizar a parada da guarda e apresentar a respetiva formatura ao oficial de dia.

Algumas Reflexões Sobre as Atribuições do Adjunto do Comandante

A ascensão ao posto de sargento-mor, que deverá ser um objetivo e a máxima aspiração de todos os sargentos, confere uma nova dimensão de responsabilidades, cujo expoente máximo julgo ser atingido com o desempenho das funções de adjunto do comandante.
Este cargo caracteriza-se por: ser um elemento do

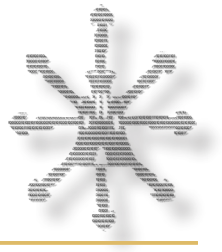
estado-maior pessoal do comandante; estar na sua dependência direta com o objetivo de que a informação flua entre ambos sem qualquer outro filtro; e ser da sua escolha pessoal, com certeza com base numa solida formação e experiência profissional, mas também pela confiança pessoal de que lhe é merecedor.



O sargento-mor, adjunto do comandante começa por ser na sua unidade a cabeça de um, ainda que informal, canal de apoio à cadeia de comando, que se estende pelos adjuntos dos comandantes de batalhão e companhia, sargento de pelotão até ao comandante de secção, através do qual são transmitidas instruções, normalmente verbais, habitualmente relacionadas com tarefas técnicas e administrativo-logísticas vitais para o funcionamento diário da unidade e com o atavio, apresentação, conduta e disciplina dos sargentos e das praças, libertando a cadeia de comando para planear, decidir e projetar o futuro.

Assumir este cargo é ter a consciência, antes de tudo, de que o seu "ethos" será, cada vez mais, o de servir. É estar ciente de que as repercussões das palavras proferidas e, principalmente, dos atos praticados, louváveis ou condenáveis, atingirão sempre com alguns estilhaços aqueles que o rodeiam.
Ser sargento-mor adjunto do comandante deverá ser, por isso, e para além das atribuições referidas nos regulamentos, fundamentalmente e sempre em primeiro lugar, dar o exemplo. Porque o exemplo tem efeitos mais duráveis do que qualquer preleção voluntarista. O exemplo na apresentação, no atavio, no comportamento ético pela prática das virtudes e valores morais e militares, como a honestidade, a camaradagem, a lealdade e o profissionalismo. É uma atitude que exige um trabalho permanente de sentinelas de nós mesmos. Como disse alguém "Vigie os seus pensamentos, porque eles se tornarão as suas palavras; Vigie as suas palavras, porque elas se tornarão os seus atos; Vigie os seus atos, porque eles se tornarão os seus hábitos; Vigie os seus hábitos, porque eles se tornarão o seu caráter; Vigie o seu caráter, porque ele será o seu destino".

Uma vez fardado desta forma, por dentro e por fora, o sargento-mor está munido da principal autoridade, a moral, para o desempenho das suas funções, designadamente para "… zelar pelo atavio, apresentação, conduta e disciplina dos sargentos e praças…". Até porque, a autoridade conferida ao sargento-mor adjunto do comandante para o desempenho das suas funções, é apenas a autoridade geral, comum a qualquer militar superior hierárquico em relação a um seu inferior hierárquico.
Penso que urge, a este propósito, integrar, regulamentarmente, o adjunto do comandante no processo de avaliação individual (AI) de todos os sargentos da sua unidade, no sentido de tornar consequente e mais eficaz esta sua ação de zelo.
Ou tendo como modelo o sistema de avaliação do exército dos EUA (Army Regulation 623-3 Evaluation Reporting System) ou de qualquer outra forma, a inclusão da avaliação do sargento-mor na avaliação individual dos sargentos, estabeleceria uma correspondência direta, coerente, responsável e responsabilizável, da sua ação de zelo e liderança e contribuiria para o fortalecimento dos laços profissionais, o incremento da motivação, da produtividade e da disciplina no seio da Institu-



ição. A manutenção do sargento-mor adjunto do comandante, desligado do sistema de avaliação dos sargentos, para além de parecer contraditório com o seu dever de "… Atuar, em nome do comandante, nos assuntos que digam diretamente respeito à categoria de sargentos…", poderá inclusive ser motivo de algum enfado pela discrepância que poderá existir entre as causas verificadas e os efeitos produzidos durante a sua ação de zelar "… pelo atavio, apresentação, conduta e disciplina dos sargentos…" e o resultado final da AI.

Ser sargento-mor adjunto do comandante é ser o seu primeiro conselheiro e consultor "…nos assuntos que digam diretamente respeito à categoria de sargentos…".
É ser como que o provedor dos sargentos. É estar atento e preocupado com os problemas, os anseios e as preocupações que afligem este grupo de profissionais que, apesar de ser cada vez mais a coluna vertebral dos exércitos modernos, pela extraordinária evolução das competências e capacidades adquiridas nas várias áreas do saber, que se têm refletido num enorme incremento da qualidade do seu desempenho e na complexidade das tarefas que lhes são atribuídas, nem sempre tem merecido o devido reconhecimento e a melhor atenção por parte da instituição.
Apenas para dar um exemplo, atente-se no tempo que tarda em certificar a sua formação.
Enquanto se reconhece, valida e certifica, há já vários anos, competências (RVCC) adquiridas ao longo da vida, através de um portfólio em substituição dos habituais anos escolares, não se reconhece, não se valida nem se certifica aos sargentos do quadro permanente (QP) as competências e as capacidades adquiridas ao longo dos anos letivos da sua formação. Os sargentos do QP ingressam no curso de formação de sargentos (CFS) com o ensino secundário concluído e terminam o CFS, passados dois ou três anos letivos, conforme os casos, exatamente com a mesma certificação académica.
A certificação da formação e o cumprimento da missão não são antagónicos. Pelo contrário. Na medida em que o processo de certificação da formação levaria necessariamente a uma melhoria da sua qualidade, ajudaria, seguramente, no cumprimento da missão.

"O sargento-mor é um elemento do comando do regimento ou do batalhão independente e desempenha as funções de adjunto do comandante para os assuntos relacionados com a vida interna da unidade, nomeadamente no que respeita à… formação dos sargentos…"
Esta formulação do RGSUE corrobora o estipulado no EMFAR e atribui ao sargento-mor a possibilidade de ser instrutor. Verifica-se, contudo, que esta tarefa tem pouca aplicabilidade, mesmo nas escolas práticas, onde seria mais plausível. Sendo natural que os conhecimentos técnicos e de carácter prático relativos ao quadro especial do sargento-mor foram ficando esquecidos nas gavetas das secretárias das companhias, dos batalhões e das secções de estado-maior, a instrução a ministrar por este deverá ser em áreas de formação teórica de caracter geral, como chefia e liderança, legislação, escrituração, etc.. Ora, sendo estas matérias apenas proporcionadas em estabelecimentos de ensino de formação base, como a Escola de Sargentos do Exército, o adjunto do comandante dessa unidade será o único com condições para desempenhar esta tarefa.
Contudo, é importante que o sargento-mor adjunto do comandante tenha conhecimento de tudo o que envolve a formação dos sargentos, quer do planeamento, quer dos conteúdos curriculares, quer da forma como é ministrada a instrução. A maneira mais ajustada de ligar mais diretamente o sargento-mor à formação dos sargentos, em especial nas escolas práticas, seria atribuir-lhe, por inerência de funções, a direção dos CFS e/ou fazer parte dos respetivos conselhos escolares.

"Nos dias de atividade normal, organizar a parada da guarda e apresentar a respetiva formatura ao oficial de dia."
Esta, que é a única atribuição de natureza diária, deixou de fazer sentido que seja realizada pelo sargento-mor, por não haver, efetivamente, parada

para organizar. Não há banda de música ou fanfarra, não há terno de clarins ou corneteiros, não há reforço, não existe ronda, não há piquete e não há mais do que um adjunto de comandante de companhia a conduzir à parada da guarda o pessoal de serviço. Esta função, que deveria consistir em organizar as forças atrás referidas, recebidas dos vários adjuntos dos comandantes das companhias, resume-se a receber a formatura do graduado que conduz o pessoal de serviço à parada e passá-la ao oficial de dia.

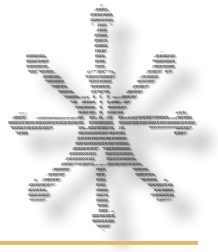
Acompanhar a vida interna da unidade (exceto nos aspetos de serviço diário e segurança) no sentido da manutenção, em alto grau, da eficiência e da disciplina;
Aparentemente uma tarefa fácil, é, porventura, a mais difícil de conseguir. Como o sargento-mor adjunto do comandante não tem por função fazer coisas, nem decidir como as fazer, é possível que tudo aconteça sem o seu conhecimento.
É imprescindível existir uma preocupação permanente do próprio adjunto do comandante, em envolver-se e do comandante em envolve-lo nos acontecimentos e no processo de tomada de decisão dos assuntos da "…vida interna da unidade…". É nesta altura que, em caso de diferentes pontos de vista, deverá apresentar os seus argumentos, com frontalidade, para que, com lealdade, uma vez tomada a decisão a deva considerar como sua. Só assim, poderá facilmente defendê-la, apoiá-la e principalmente justificá-la sendo, genuinamente, um agente motivador para os que o rodeiam. A mobilização do sargento-mor adjunto será tanto maior quanto mais se sentir envolvido e corresponsabilizado no processo de decisão e empenhado na sua realização.
Sempre que um comandante visita uma das unidades ou subunidades que comanda, ou qualquer acontecimento, deverá ter a preocupação de se fazer acompanhar do seu sargento-mor adjunto. Ao fazê-lo estará a proporcionar-lhe o tal acompanhamento da vida da unidade e o contacto com os sargentos e as praças inteirando-se do seu estado de espírito, do grau de disciplina e das suas preocupações, transmitindo, simultaneamente, um sinal de coesão do comando e de consideração pelos sargentos e pelas praças.
Com esta postura o comandante evitará os simpáticos mas ineficientes "Oh mor, desculpe lá! Esqueci-me de si!", e o sargento-mor o irresponsável, indouto e desmobilizador, "Eles…". Qualquer das formulações com consequências nefastas para a motivação e o estado de espírito do pessoal da unidade.

Conclusões

Como se pode verificar, do RGSE de 1980 ao RGSUE de 2005, as funções do sargento-mor adjunto do comandante sofreram uma enorme transformação. As atribuições explícitas, de carácter executivo, com influência direta no desenrolar da vida interna e diária da unidade deram lugar a um quase completo vazio de conteúdo. E se é natural que à medida que aumenta o posto e o cargo diminuam os deveres discriminados e aumentem os implícitos, também é suscetível de, se não houver a devida compensação e atenção, o cargo se tornar, desmotivador, desinteressante e numa figura meramente decorativa, onde não será possível encontrar qualquer realização profissional.

As atribuições dos cargos congéneres dos exércitos analisados são muito similares. São sempre em primeiro lugar os conselheiros diretos dos comandantes nos assuntos relacionados com os sargentos nuns, sargentos e praças noutros, e intervenientes ativos nos aspetos do atavio, apresentação, conduta, disciplina e formação dos sargentos e das praças. As diferenças fundamentais residirão na consideração, no respeito e nas condições disponibilizadas para o seu desempenho.

Quer no exército dos EUA, desde 1966, quer no exército espanhol, desde 2006, foi criado o cargo "sargento-mor do exército". Qualquer deles toma



posse em cerimónia própria para o efeito, tem autonomia para promover contactos e reuniões com os adjuntos dos comandantes dos escalões subordinados, desenvolve a sua função em gabinete próprio, habitualmente na área do gabinete do respetivo comandante.
Ambos têm ainda a incumbência de serem porta-voz dos assuntos relacionados com os sargentos e as praças nas mais altas instâncias. Em Espanha o rei Don Juan Carlos, nas suas habituais audiências militares, recebe anualmente comissões constituídas por sargentos-mores dos vários ramos das forças armadas e forças de segurança, para os ouvir sobre os assuntos que os concernem. De igual modo, uma das atribuições explícitas do sargento-mor do exército dos EUA é comparecer perante o congresso para falar sobre os assuntos que digam respeito aos sargentos e às praças.

Passados trinta e seis anos sobre a criação do cargo de sargento-mor adjunto do comandante, penso que existe ainda um longo caminho a percorrer, que terá sempre como farol o cumprimento da missão e o prestígio da instituição militar, no sentido de uma melhor assimilação e compreensão pela hierarquia, tendente a um maior envolvimento na vida da instituição, em consonância com as suas capacidades, competências e experiência profissional.



MGen Pinto de Castro

Entrevista realizada pelos Alferes TPO Tiago Santos, João Monteiro e Humberto Costa.

Introdução

Como tem vindo a ser tradicional, entrevistámos na presente edição da revista A Mensagem, mais uma destacada figura da Arma de Transmissões. Este ano procurámos descobrir um pouco mais do percurso militar e pessoal do Exmo Senhor General Pinto de Castro. Agradecemos a disponibilidade do Exmo Senhor General, bem como a frontalidade e abertura patenteadas no decorrer da entrevista.

1. O que levou o meu General a seguir a carreira militar?

"Gosto pela vida militar e em especial na área da engenharia eletrotécnica. Quando estava ainda no liceu já gostava de brincar com a eletrónica e radio amadorismo."

2. Uma vez ingresso na carreira militar, o que levou o meu General, em determinada altura, optar pela arma de Transmissões?

"Desde jovem, sempre gostei de eletrónica seguindo e acompanhando as iniciativas de radioamadorismo o que me levou a ver nas Transmissões a possibilidade de tirar o curso de eletrotecnia e assim concretizar o meu sonho. Quando concorri à AM – Academia Militar, já tinha feito com êxito o exame de aptidão ao curso de eletrotecnia do IST – Instituto Superior Técnico. Na altura não se escolhia logo transmissões, escolhia-se engenharia e ao fim do primeiro ano escolhi transmissões que era aquilo que realmente gostava, eletrotecnia."

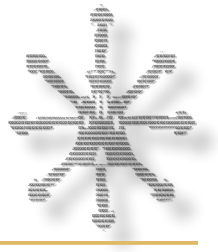
3. Sabemos que por imposição de serviço foi nomeado para uma comissão no ultramar, em Angola. Pode recordar-nos quais os principais desafios que enfrentou neste teatro de operações?

"No ATA, estive 6 meses como continuação do tirocínio. Durante esse período, tive como principais missões: pôr a funcionar um emissor de 500 KW da Racal do STM e montar dois rádios de HF, um em Carmona e outro em Belize em Cabinda, para melhorar a rede do STM em Angola."

4. Qual a importância das Transmissões no teatro de operações em Angola?

"As Transmissões da Rede Fixa (STM) foram decisivas para garantir o Comando e o Controlo das várias Operações desencadeadas no TO, assim como as Transmissões de campanha das Unidades foram fundamentais para acompanhar as patrulhas, comboios logísticos e operações efetuadas em áreas muito grandes de dezenas ou centenas de Quilómetros. Servia para o comando e controlo a partir de Luanda em HF"

5. Aquando o regresso do meu General da comissão no ultramar, foi colocado na EPT – Escola Prática de Trans-



missões como capitão. Durante os quatro anos de colocação nesta unidade qual ou quais as contribuições pessoais mais significantes para as Transmissões?

"Fui colocado no Serviço de Fx Hz onde acompanhei a montagem do link Sul desde a EPT, Palmela, Mendro até Évora. Participei no 25 Abril 74 e a seguir fui nomeado adjunto do Diretor técnico da RTP."

6. Qual o empenho do meu General nos movimentos das Forças Armadas no dia 25 Abril de 1974?

"Antes do 25 Abril fiz parte da Comissão Coordenadora do MFA. Durante a Operação estive na EPT onde tinha a missão de estabelecer uma ligação em HF entre a EPT e o RT no Porto, a qual falhou por avaria do E/R RF-301 destinado à ligação. Tinha um PA muito sensível e falhou. Em face disso segui para a Central Telefónica Militar a fim de colaborar na interseção das chamadas efetuadas."

7. Durante a colocação do meu General na Brigada Mecanizada Independente qual era a situação das comunicações de campanha?

"A CTm da Brigada era um local de excelência porque era o único local onde se podia trabalhar operacionalmente. Naquele tempo a Grande Unidade designava-se por BMI – Brigada Mista Independente. Nessa altura, as Transmissões de Campanha estavam a mudar o seu conceito de funcionamento, que era integrado nas Transmissões Permanentes, para um funcionamento em separado como Transmissões Táticas. Tinham o seu centro de especialização para o material de Transmissões no Depósito Geral de Material de Transmissões em Linda-a-Velha e para a doutrina na EPT, já no Porto, e o IAEM. Entretanto, a Companhia de Transmissões na BMI, seria a Unidade de Transmissões Operacional de excelência, pois, por ter meios e por estar enquadrada numa Grande Unidade com excelente Capacidade Operacional era o local ideal para os Oficiais de Tm poderem aplicar e executar as doutrinas aprendidas. Naquele tempo a Companhia de Tm só tinha meios filares para montar a rede telefónica, não existiam ainda os meios de Fx Hz."

8. Mais tarde em 1989 o meu General é nomeado coordenador do projecto de desenvolvimento de protótipos de E/R VHF portátil de 30 a 88 MHz. Em que consistiu o projeto?

"Penso que se estão a referir ao desenvolvimento do P/PRC-501. Era uma evolução do P/PRC-425 que foi o primeiro equipamento que se desenvolveu em Portugal para o Exército. Ou seja, como o desenvolvimento é contínuo porque após a conclusão de um protótipo, surgem logo ideias para um novo modelo mais evoluído e com melhores possibilidades, aconteceu que a seguir à conclusão do projecto do P/PRC-425 que só trabalhava numa faixa de 10 MHz, pôs-se logo a questão de, a partir dele, desenvolver um equipamento mais miniaturizado e com mais possibilidades, inclusive no número de canais, e que pudesse vir a substituir o AVP-1, muito grande e limitado para as ligações de Pelotão/Secção, surgindo então o P/PRC-501.
Ora, aconteceu que tive a possibilidade de integrar a equipa que desenvolveu o P/PRC-425 com funções executivas como os outros elementos militares da equipa, tendo-me calhado a responsabilidade de conceber e desenvolver Painel Frontal com a respetiva placa eletrónica e o Filtro de Antena.
Entretanto, como naquele tempo a filosofia da DAT – Direção da Arma de Transmissões, era fazer o reapetrechamento das Transmissões Táticas do Exército a partir de equipamentos desenvolvidos pela Indústria Nacional, e como eu na altura integrava os quadros do DGMT, chegando a ser Diretor, pude ter a felicidade de acompanhar e coordenar" uma série de projetos, dos quais, destaco os mais importantes, como por ex-

emplo, toda a família do P/PRC-425, as Centrais Telefónicas Digitais, o E/R de HF P/VRC-301, um Carregador de Baterias de Carga Rápida, vários tipos de Cabines de Transmissões, um Mastro Telescópico, um Terminal Tático de Comunicações, o Interface Criptofónico, o Sistema Intercomunicação para Carros de Combate., o Telefone de Campanha P/BLC-101, etc.
Saliento ainda o Terminal de Satélite PoSat P/USC-701 com o qual o Exército realizou pela primeira vez as ligações via satélite, através do satélite português PoSat 1, entre o RT e a CTm5 em Angola."

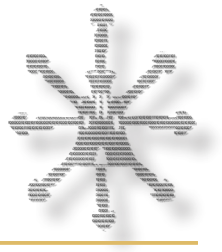
9. O meu General foi comandante do BTm 4. Quais as principais dificuldades na constituição deste Batalhão?

"A primeira dificuldade, prendeu-se desde logo com a conceção e dimensionamento de uma Unidade apropriada para dar resposta aos requisitos definidos pelas NU nas suas "Guide Lines" relativos à sua sustentabilidade e à da Missão Operacional de Transmissões, já que, no Exército não existia nenhuma Unidade de Transmissões Tática do tipo Batalhão. Por isso, e pelo fato de ser a primeira vez que Portugal participava numa Operação Externa com uma unidade do tipo Batalhão, não havia experiência nem doutrina sobre o assunto. Foi necessário desenvolver um grande trabalho de estudo e dimensionamento em todas as áreas, quer técnicas de transmissões quer logísticas, com a realização de inúmeras reuniões onde participaram elementos de todas as áreas logísticas do Exército.
Os requisitos mais importantes a ter em consideração, eram, em termos logísticos, o fato de a Unidade ter que ser autossustentada durante 60 dias (que era o tempo estimado pelas Nações Unidas para implementar o Sistema de apoio Logístico da força ONUMOZ e, em termos de Transmissões, o fato de garantir a ligação em fonia, TT e Dados entre as Zonas Militares tão distantes entre si, cerca de 1200 Km.
A segunda dificuldade prendeu-se com a seleção, nomeação e formação do pessoal, especialmente o de natureza técnica, visto que, a Unidade teria que montar, instalar, explorar e manter o Sistema de Transmissões planeado por Portugal e aprovado pelas Nações Unidas.
Salienta-se que a participação de Portugal nesta missão só foi possível porque coincidiu com o fim de fabrico de uma série de meios, que a DAT tinha encomendado à Indústria Nacional tendo em vista, precisamente a criação de um Batalhão de Transmissões Tático e que foram já referidos atrás. Por essa razão quase todo o material de transmissões deste BTm4 era de fabrico Nacional, incluindo os equipamentos multicanal E/R FM 200 e o multiplexer DX 15-60, fabricados sob licença em Portugal. Só não eram de fabrico Nacional os terminais de satélite INMARSAT e as antenas logarítmicas de HF."

10. Porquê o nome BTm 4? Quais as principais dificuldades sentidas no TO?

"O nome de BTm4 foi decidido pelo EME por já terem existido os Batalhões 1,2 e 3 das Divisões 1,2 e 3.
Durante a Operação, das várias situações onde se sentiram dificuldades, destaco o momento da instalação do BTm e o momento em que as NU exigiram um redimensionamento do Batalhão para a concretização de uma política de redução geral dos efetivos da Força da ONUMOZ antes da fase das eleições."
As dificuldades durante a instalação prenderam-se com a demora dos funcionários da NU em escolherem um espaço adequado para o acampamento e com o facto de não disponibilizarem os meios estruturais de apoio prometidos, o que levou a estar bastante tempo sem as condições mínimas de funcionamento.

11. Em 1987 e em 1994, o meu General foi membro do Concelho para a Arma de Transmissões. Qual a evolução da arma neste período? E quais os principais desafios colocados à arma?
"É um período em que se acentua o vetor das transmissões táticas que tinha começado em 1974. Até àquela



data as transmissões viviam um conceito de transmissões de campanha que funcionava imbuída nas transmissões permanentes, com o pessoal a operar nas duas áreas em função das necessidades. A partir daquela data, as transmissões, assim como o Exército, reestruturaram-se para se integrarem em Unidades Táticas preparadas para uma Guerra Convencional, o que em termos de transmissões obrigou a pensar em meios a utilizar em TO convencionais, significando que se deveria pensar no reequipamento das unidades do Exército com meios de VHF em vez de meios HF. Por isso, a DAT começou a apostar numa separação entre as transmissões táticas das permanentes, transformando o DGMT num centro muito especializado dedicado à aquisição, conceção, sustentação e manutenção dos meios de transmissões táticos e a EPT dedicada à doutrina das transmissões táticas e à condução da Guerra Eletrónica."

12. Sendo a década de 90 o marco de evolução dos sistemas informáticos, de que forma estes influenciaram, na sua perspectiva, o papel das Transmissões (Segurança, Sistemas de Informação, etc..)?

"Os meios informáticos marcaram decisivamente a mudança de atuação das transmissões. A mudança foi na conceção do Comando e Controlo que passou a funcionar assente numa rede de dados no TO e que alterou completamente o antigo lema de "Levara Carta a Garcia" para talvez um novo lema de "Levar a Ficha a Garcia". Com os dados a fluir na rede é possível ter a funcionar um Sistema de Informação, um Sistema de Controlo de Meios, um Sistema de Comando, sendo ainda possível incluir Sistemas de Segurança mais fiáveis e duros. Por outro lado, a informática administrativa passou a ser também da área das transmissões, o que é logico para não se dispersar meios e responsabilidades, aumentando assim o papel e a influência das transmissões no Exército."

13. Das várias condecorações recebidas pelo meu General, qual é aquela que para o meu General tem mais significado?

"A medalha que teve para mim mais significado, foi a Medalha de Serviços Distintos de Prata recebida na sequência da Operação da ONUMOZ, não só pela honra de a ter recebido, mas também pelo reconhecimento do meu desempenho numa missão que apesar de difícil, foi estimulante pelo desafio enorme que representou e pelo prazer que proporcionou.
Não posso deixar de dizer que tive um grande prazer por ter recebido a Medalha de Mérito Militar 2ª Classe como reconhecimento pela minha participação técnica no desenvolvimento do P/PRC-425"

14. Face a uma experiência militar e humana tão rica e diversificada estamos, certos que passou por diversas situações caricatas, em que foi colocada à prova a sua capacidade de liderança. Pode revelar-nos sucintamente uma dessas situações?

Lembro me de uma situação durante a formação do Batalhão, estava eu a chegar de Moçambique, após efetuar um reconhecimento no TO, quando fui informado que todo o pessoal que se tinha voluntariado para a missão estava á minha espera, no sentido de me manifestarem o seu descontentamento, por causa das ajudas de custo a receber durante a missão. A situação estava de alguma forma tensa, chegando mesmo a existir ameaças de desistência da missão. Os militares do Batalhão tinham sido informados que as ajudas de custo a receber, que julgavam serem equivalentes ao do Corpo Diplomático e que foram pagas a alguns militares que estiveram em ações de cooperação em Angola, afinal seriam muito menores.
Apos um reunião com o CEME aonde foi possível uma melhoria das ajudas de custo, dirigi-me ao RTm onde

estava todo o pessoal reunido e em conversa com eles, entre várias razões que evoquei para os demover da ideia, disse-lhes ser evidente que o Governo não iria dar o mesmo montante a um efetivo de Batalhão como deu a um pequeno grupo e que achava incompreensível que gente tão nova, sedenta de aventura, estivesse mais preocupada com o dinheiro, do que com a oportunidade de participar numa missão única na vida. Ao fim de mais alguma troca de argumento de parte a parte, a rapaziada nova e velha todos estavam prontos a participar na missão.

15. O País atravessa um período difícil. Como é que o meu General, com a sua vasta experiência de vida, observa este período? Nomeadamente no que diz respeito a possíveis consequências para o Exército e mais especificamente para as Transmissões?

A minha experiência diz-me que Portugal como membro da NATO, não pode deixar de dar o seu contributo com Forças para as missões de Paz em que a NATO se empenha, assim como também terá que contribuir com Forças para as Missões do âmbito Europeu.
Desse modo, penso que o Exército, embora tenha que sofrer grandes constrangimentos por força das dificuldades económicas, vai ter que ter sempre uma ou mais Grandes Unidades Operacionais para poder dar uma resposta mínima às nossas obrigações externas.
As transmissões são sempre necessárias para montar o Sistema que garanta o exercício de Comando e Controlo, quer das Grandes Unidades e Pequenas Unidades táticas, quer das transmissões permanentes, e portanto, acho que vão ter que continuar a existir as Unidades Atuais.
As transmissões perderam e vão continuar a perder a Capacidade Técnica relativamente ao material de transmissões em geral. Isto, porque a adoção do conceito de "Outsourcing" pelo Exército, que considero um grande erro, conjuntamente com a integração da Logística, tem levado cada vez mais, a uma menor intervenção das Transmissões quer na manutenção, quer no desenvolvimento e reabastecimento. Consequentemente as Transmissões vão-se transformando num utilizador puro e simples dos meios sem qualquer possibilidade de neles intervir ou até de os perceber profundamente.
Na área Digital e Informática as Transmissões têm tido elementos bem preparados e com uma boa capacidade de intervenção nos sistemas, levando a crer que essa capacidade melhorará nos próximos anos.

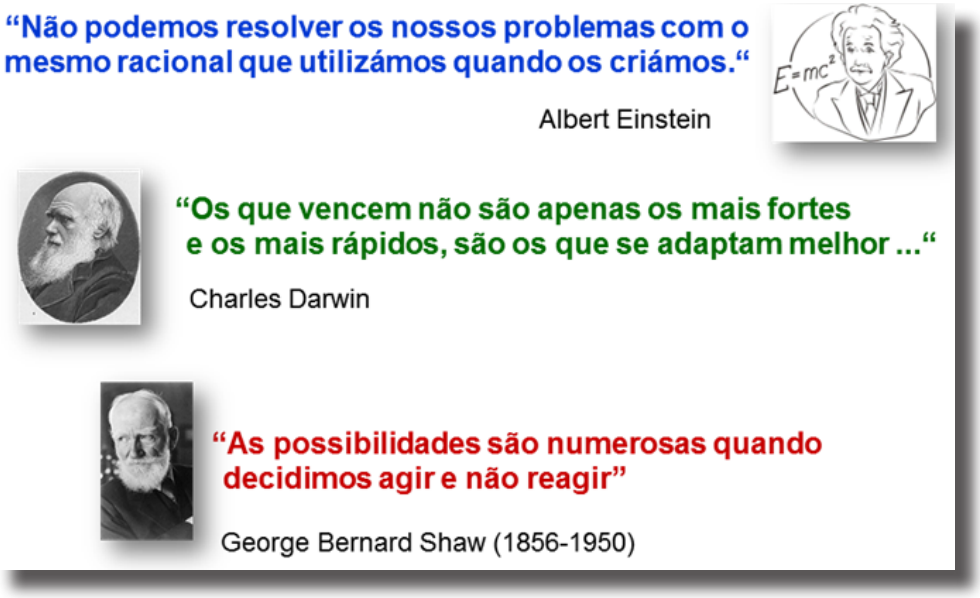
16. Que mensagem gostaria de deixar para todos os jovens militares presentes nas Forças Armadas e em específico para os recém-chegados à Arma de Transmissões?

Desejo dizer aos jovens militares que cultivem as virtudes militares e se dediquem e empenhem de forma franca, leal e generosa, como sempre tem acontecido, à causa Militar e à Pátria porque é isso que a Nação espera deles. Peço-lhes também que acreditem e tenham esperança, porque embora se vivam hoje tempos difíceis, eles serão efémeros e passageiros e é preciso estar prontos e preparados para quando a Nação chamar por eles.
Os jovens chegados às Transmissões devem estar cientes que as Transmissões são cada vez mais importantes nas Forças Armadas e que eles têm um papel importantíssimo no êxito do Exército ao terem que manter a eficiência do Sistema de Transmissões que garanta o Comando e Controlo.

Superioridade de informação no Exército. Um objetivo estratégico



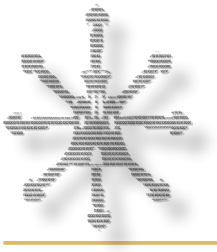
Maj Tm (Eng.) Luís Carvalho



Introdução

As Forças Armadas, à luz da Constituição da República Portuguesa, constituem o corpo social responsável pela defesa do Estado contra ameaças externas e devem assegurar, em situações de exceção (e.g. estado de sítio), o regular funcionamento das instituições democráticas e o exercício das funções de soberania do Estado. Face à natureza assimétrica e transversal da ameaça, onde se torna difícil clarificar a origem (interna ou externa) e o impacto dos ciberataques, as Forças Armadas deverão também assegurar o desenvolvimento de capacidades e assumir competências no domínio da ciberdefesa, nomeadamente, as que permitem contribuir para proteger as infraestruturas de informação críticas e o governo eletrónico do Estado.





Superioridade de informação no Exército. Um objetivo estratégico

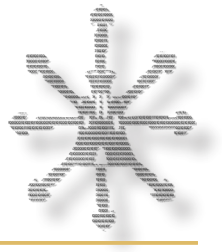
A evolução do ambiente estratégico, em curso, aponta de forma clara para a emergência da Guerra de Informação como um novo paradigma da Guerra e, neste âmbito, para um incremento da importância das Operações de Informação na condução dos futuros conflitos. Os responsáveis pela área do planeamento militar, têm vindo progressivamente a tomar consciência deste facto, desenvolvendo estratégias e capacidades destinadas a preparar as Forças militares para o envolvimento em guerras no domínio da informação de larga escala[1]. Neste âmbito, será de esperar que no curto/médio prazo venha a ser também atribuída às Forças Armadas a responsabilidade de colaborar e cooperar na garantia da Ciberdefesa do País, onde todas as atividades conduzidas no domínio da Informação, tanto na área CSI como na área da Guerra de Informação, passam assim a requerer uma gestão (horizontal e vertical), coordenada e integrada ao mais alto nível, de forma a sincronizar e a maximizar o impacto dos efeitos a produzir no ambiente de informação. Também ao nível da Segurança da Informação, é possível constatar que as políticas de segurança foram no passado sempre baseadas no princípio de "evitar o risco". Esta aproximação, encontra-se no entanto desajustada da realidade, devendo a proteção ser cada vez mais orientada para a sua gestão. Assim sendo, o nível do risco[2] deve ser mantido razoavelmente baixo, nomeadamente, através do levantamento de capacidades associadas à Information Assurance (Ciberdefesa e INFOSEC). Perspetivando-se de certa forma a tendência para um aumento das ciberameaças, no âmbito nacional como internacional, importa também equacionar o desenvolvimento de uma capacidade de proteção e defesa neste domínio, clarificando os aspetos ligados à Cibersegurança, de responsabilidade generalizada e transversal, dos que, por colocarem em risco a Segurança e Defesa do Estado, se enquadram no domínio da Ciberdefesa, exigindo uma participação ativa e clara das Forças Armadas.

Uma vez que a ciberdefesa do País, consubstanciada através da proteção das infraestruturas críticas nacionais, só se poderá obter com base no desenvolvimento de Operações de Informação Defensivas e com o contributo indispensável das Forças Armadas, estas capacidades deverão ser geradas com base no princípio de "duplo-uso". Com este artigo pretende-se dar a conhecer os últimos desenvolvimentos do Exército no levantamento da Capacidade de "Superioridade de informação", um objetivo estratégico para o Exército. Para isso o artigo foi desenvolvido em sete capítulos. Depois da introdução fez-se um enquadramento procurando fazer um ponto de situação da realidade atual, para depois caracterizar os riscos e os desafios da atualidade, onde se pretende mostrar a mudança de paradigma. No terceiro capítulo abordou-se a superioridade de informação para depois se traçar a Visão e o Plano de Ação. No sexto capítulo são caracterizados os vetores desenvolvimento Organização e Pessoal para no sétimo capítulo serem referidos os próximos passos que devem ser dados no levantamento desta capacidade, para terminar com umas breves conclusões.

1 Os recentes ciberataques conduzidos contra a Estónia (Abril/Maio de 2007) e contra a Geórgia (Agosto de 2008), constituem bons exemplos do que aqui se refere.

2 Dado o novo espectro da ameaça, uma política dinâmica de gestão do risco é absolutamente necessária para obtermos sistemas que apresentem um nível de segurança apropriado ao desenvolvimento de uma gama alargada de tarefas, que sejam financeiramente sustentáveis e funcionalmente eficazes.

Superioridade de informação no Exército. Um objetivo estratégico



1. Enquadramento

O sector das Tecnologias de Informação e Comunicação (TIC)[1] tem um conjunto de características específicas que o diferenciam dos sectores de atividade no sentido convencional do termo, não só porque se trata de um sector baseado na ciência, mas também pela sua enorme flexibilidade, o que faz com que seja transversal a um grande leque de atividades organizacionais (e.g. social, política, económica e militar) e também domésticas. As TIC, com a sua linguagem isotérica e as suas concretizações em termos de aplicações, bases de dados, redes e sistemas operativos, que suportam e instrumentam as organizações, são constituídas por Entidades Informacionais, por Fluxos Processuais, por Pontos de Decisão e por Meios de Atuação. É neste referencial que os seres humanos se situam em relação às TIC, pois cada um de nós num dado momento e num certo contexto (fluxo), tendo em conta a problemática concreta (informação) toma a decisão de agir de determinada forma (atuação). É por isso que nos próximos anos, devido à rápida evolução das TIC, as Forças Armadas passarão a ser condicionadas pela necessidade crescente de potenciar a utilização de novas formas de organização, arquiteturas e plataformas tecnológicas que fornecerão os alicerces para uma maior eficiência e eficácia operacional. O futuro apresenta-se bastante promissor em termos de evoluções, que ainda não podemos prever neste momento, mas que prometem mudanças de paradigma e, sobretudo cada vez mais no caminho da banalização da utilização dos sistemas e tecnologias de informação e comunicação. A emergência de novos modelos de interação global, acompanhada pelos recentes sinais de exploração militar da Internet e do Ciberespaço[2], tem também um impacto profundo no ambiente estratégico internacional, não só ao nível político, económico e social mas também ao nível militar, daí resultando inevitáveis implicações para a atividade das Forças Armadas. Dentro deste contexto, o Ciberespaço constitui hoje o 5º domínio operacional, reconhecido por vários países da OTAN e EU, materializando um novo campo de batalha onde têm lugar operações militares destinadas a moldar o ambiente de informação, de acordo com a salvaguarda dos interesses dos Estados. Assim, constata-se que a forma como os diferentes atores utilizam a informação pode ser simultaneamente geradora de novas oportunidades e de novas ameaças no ciberespaço, apresentando importantes implicações na condução da política e da estratégia dos Estados. Isto obriga a que os Estados mantenham o empenhamento das suas capacidades de cibersegurança e ciberdefesa nos diversos teatros (reais e virtuais). Neste contexto, a componente não cinética dos conflitos tem vindo a assumir uma especial preponderância, colocando importantes desafios às Forças Armadas, num mundo virtual informático que constitui, cada vez mais, o habitat operacional onde as ações dos seus agentes se concretizam, e onde têm que levantar as capacidades necessárias para uma atuação eficaz em novas dimensões do moderno campo de batalha, nomeadamente no domínio da Informação e do Ciberespaço. Podemos assim afirmar que a evolução do ambiente operacional e a natureza dos futuros

1 Por TIC designamos hoje todo um conjunto de artefactos tecnológicos com que instrumentamos o habitat humano, que facilitam e aumentam as capacidades individuais e coletivas na comunicação, na recolha, no tratamento, na preservação de informação e no suporte às ações que desencadeamos em consequência das decisões que tomamos, nos diversos contextos em que nos situamos ao longo do tempo (Tribolet, 2011: 8).

2 A palavra "Ciberespaço" resulta da associação dos termos "cibernética" e "espaço". Tendo sido inicialmente utilizada pelo escritor canadiano William Gibson, no seu livro "Neuromencer" (1984), a sua utilização viria mais tarde a generalizar-se para descrever o espaço virtual associado à Internet. Atualmente, face às diferentes visões e interpretações sociológicas que o Ciberespaço suscita, é nossa convicção, que o seu estudo poderá ser sistematizado segundo duas perspetivas (Nunes, 2010): como infraestrutura tecnológica de informação, composta pela interligação física de redes de computadores que constitui a World Wide Web; como espaço virtual, palco de interações sociais, económicas, políticas e culturais.



cenários de empenhamento das Forças Armadas, obrigam a rever o paradigma atual, em que a informação não é ainda perspetivada de forma global e integrada, na sua dupla vertente de recurso/arma. Este novo enquadramento, com um importante impacto na atividade das Forças Terrestres, estrutura-se de acordo com a visão do Exército como uma Organização em Rede, onde a obtenção da Superioridade de Informação é considerada um fator-chave, determinante do sucesso operacional.

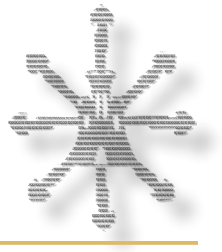
2. Riscos e desafios da atualidade

A universalidade da atividade humana, suportada por uma sociedade em rede, constitui uma das características fundamentais deste novo século. Vivemos num mundo interdependente, onde a crescente conectividade das infraestruturas de informação impulsionou o surgimento de uma rede de cobertura mundial. Com a utilização massiva da Internet, assistimos a uma alteração significativa tanto da natureza das ameaças como do nível dos ataques maliciosos (perpetrados por hackers, organizações criminosas, organizações e movimentos terroristas e os próprios Estados) dirigidos contra os sistemas integrados em rede. Estes sistemas e os seus elementos estruturais constituem a componente tangível de um espaço virtual a que atribuímos a designação de ciberespaço. Diferentes atores podem explorar o ciberespaço de forma competitiva ou hostil para atacar as infraestruturas de informação que apoiam a atividade das Forças Armadas e das Forças de Segurança. Dependendo da sua natureza e do grau de disrupção estimado para a sociedade, estes ataques podem colocar em risco as infraestruturas críticas, consideradas vitais para a sobrevivência das "Sociedades da Era da Informação". Esta situação, para além de afirmar a emergência de novas ameaças, impõe aos Estados o levantamento de uma Estratégia da Informação, obrigando-os a rever e a alargar o foco do seu conceito de Segurança e Defesa, nomeadamente, de forma a incluir o ciberespaço como um novo domínio de projeção de poder. A crescente militarização da Internet vêm assim suscitar uma preocupação redobrada pois não é possível ignorar que os ciberataques lançados ou patrocinados por Estados são aqueles que apresentam um maior poder disruptivo. Neste quadro, importa referir que o equilíbrio estratégico obriga os Estados a desenvolver capacidades de Ciberdefesa pois só desta forma será possível combater os poderes emergentes neste domínio. Neste âmbito, na revisão do seu conceito estratégico ocorrida em Lisboa (19-20 de Novembro de 2010), a OTAN incluiu já esta preocupação, considerando prioritário o desenvolvimento de uma capacidade de Ciberdefesa no seio da Aliança Atlântica. Aumentado a capacidade de prevenir, detetar defender e recuperar de ciberataques, e a capacidade de coordenação nacional na área da ciberdefesa. As recentes ações de ataques através do ciberespaço (inovações já deste milénio) à Estónia e Geórgia, ou mais concretamente o hacktivismo[1] - social, defacement, DDoS[2] (Distributed Denial of Service) ou vírus informático[3] - que tem assumido uma importância crescente nos nossos dias, com as tentativas constantes das autoridades governamentais e cooperativas de tentar combater este fenómeno, colocam desafios e reformulações das estratégias de segurança e defesa dos Estados. É neste campo que as Forças Armadas poderão

1 hacktivismo resulta da fusão entre hacking e ativismo e pode ser definida como a utilização do hacking para atingir um objetivo político ou social.

2 Ataques distribuídos de negação de serviço.

3 No social, o perito informático coloca as suas competências sociais ao serviço da comunidade; no defacement (por vezes também chamado de graffiti eletrónico) são alteradas as imagens ou o aspeto das páginas de internet para deixar algumas mensagens de teor político ou social; no mais musculado feito através dos ataques DDoS faz com que um site ou serviço Web funcione com limitações ou deixe de funcionar totalmente; na mais extrema é feito o desenvolvimento de determinados vírus informáticos que podem ser utilizados para fins políticos.



desempenhar um papel de enorme relevância, com estruturas para fazer face a esta nova realidade, numa ótica de serviço público e de salvaguarda dos interesses do Estado, assumindo-se como elemento gerador de futuras capacidades de duplo uso Civil-Militar, no quadro do desenvolvimento de uma Estratégia Nacional. Ainda que estas atividades não configurem um envolvimento direto de Estados ou organizações terroristas, já em Fevereiro de 1998 existiam indícios de que algumas organizações extremistas islâmicas estavam a procurar desenvolver uma rede de hackers[1], tanto para apoiar as suas atividades correntes como para preparar o lançamento de futuros ataques de Guerra de Informação (Denning, 1999). À medida que o espaço cibernético foi envolvendo maior diversidade de atores, passando de um círculo restrito de cientistas e militares (década de 60 e 70) para empresas (década de 80) e sociedade em geral (a partir da década de 90), a proteção das infraestruturas críticas de informação tornou-se não só uma necessidade como um imperativo (Caldas, 2011). Diversos relatórios internacionais (Deloitte, 2010; Richardson, 2011) têm sustentado a relevância deste assunto e uma crescente preocupação com esta temática no seio das organizações civis e militares. Preocupação essa atualmente acrescida pelos inúmeros métodos de ataque que podem ser realizados através do ciberespaço ou seja mais especificamente através da internet (CSO, CERT, & Deloitte, 2010; ENISA, 2011; GTISC,2010) e que são ampliados na sua importância pelas notícias que constantemente são publicadas nos media nacionais e internacionais. O elemento central nesta temática é a informação, como ativo de negócio fundamental para a organização e que necessita de ser convenientemente tratada e protegida. A informação é neste momento um ativo estratégico das organizações, na medida em que lhe permite uma melhor qualidade da sua gestão, dos seus ativos, assim como na medida em que lhe permite uma melhor qualidade da sua gestão, dos seus ativos, assim como poder implementar iniciativas que lhes podem trazer vantagens competitivas relativamente à sua concorrência. A informação é a base, para além da sua utilidade operacional permite às organizações tomarem a melhores decisões e gerirem de uma forma mais eficiente e eficaz. A qualidade dessa informação assume aqui um papel de grande relevância, tendo que ser evitada a todo o custo a sua duplicação e muitas vezes incorreções, que tem a ver com o facto de existirem nas organizações várias aplicações a gerirem a mesma informação, mas não da mesma maneira. Constituindo o funcionamento em rede e a exploração intensiva dos recursos de informação uma condição essencial ao funcionamento das modernas Sociedades e das Forças Armadas Portuguesas, o Exército pretende, através de uma atuação sincronizada no domínio da informação, potenciar a sua Capacidade de Comando e Controlo (C2) e garantir, de forma eficaz, a operação e defesa das suas redes de Comunicações e Sistemas de Informação. Tendo por base o desenvolvimento e exploração de uma capacidade residente de Guerra de Informação, consubstanciada através da condução de Operações de Informação (OI), de Operações em Redes de Computadores (Computer Network Operations – CNO) e da implementação de mecanismos de Garantia da Informação (Information Assurance – IA) [2], pretende-se também o levantamento de uma capacidade de Ciberdefesa. Neste contexto, segundo uma perspetiva de duplo-uso, o Exército poderá trabalhar em conjunto com outros atores relevantes neste domínio, contribuindo desta forma para, colaborativamente, melhorar a proteção e coordenar a defesa das Infraestruturas de Informação Críticas Nacionais, desenvolvendo e reforçando cooperativamente a capacidade de Ciberdefesa do País.

1 De acordo com o testemunho de Clark Staten, Director Executivo do Emergency Response & Research Institute de Chigago, proferido em 24 de Fevereiro de 1998, perante o Subcommittee on Technology, Terrorism and Government Information do U.S. Senate Judiciary Committee.

2 Esta Capacidade é vista pela NATO como resultando do desenvolvimento integrado da Segurança da Informação (Information Security – INFOSEC) e de Operações de Ciberdefesa.



3. A Superioridade de Informação

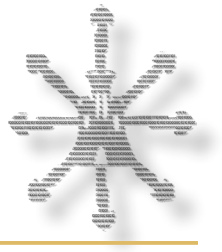
A Superioridade de Informação[1] , constitui um objetivo estratégico a levantar pelo Exército, materializando uma nova capacidade. Esta capacidade, estrutura-se com base na gestão de topo do domínio da informação, coordenando e facilitando o alinhamento do apoio CSI com a área da Guerra de Informação. Neste contexto, os recursos já existentes, constituem um importante "ponto de partida" uma vez que permitem, desde logo, identificar as componentes sobre as quais se irá edificar a nova capacidade. Através da implementação deste conceito, que envolve Pessoas, Informação e Tecnologia, será possível melhorar a eficácia operacional das Forças Terrestres com base em decisões cada vez mais rápidas e acertadas, em resultado da disponibilização da informação necessária, no momento certo e de forma segura, a todos os níveis e escalões hierárquicos. Não se trata de fazer mais coisas, mas de fazer melhor as coisas.

Tendo em vista preparar o Exército para enfrentar todo o espectro de operações e as novas dinâmicas que o moderno campo de batalha encerra, o Exército tem promovido a revisão do Apoio CSI segundo uma filosofia de Força Centrada em Rede (seguindo os requisitos NATO Network Enabled Capability - NNEC), aprovando o enquadramento doutrinário apresentado para a área da Guerra de Informação e definindo princípios de coordenação do domínio da informação. Neste contexto, a capacidade para gerir a mudança e para definir uma gestão de topo, capaz de integrar e coordenar os processos que permitem intervir de forma coerente e eficaz no ambiente de informação, constitui uma condição necessária para empreender um esforço estrutural tão importante como o levantamento de novas capacidades e a transformação de outras já existentes. Reconhecendo as vantagens de, numa altura de graves restrições de recursos financeiros e humanos, reduzir ao máximo o impacto do levantamento desta capacidade na sua atual estrutura, o Exército tem vindo a refletir sobre um conjunto de ajustamentos orgânicos que passariam, nomeadamente, pela consolidação e criação no curto prazo de:

- **Um Centro de Operações de Informação** que, funcionando como elemento coordenador das diferentes atividades conduzidas pelo Exército no domínio da informação (Operações em Redes de Computadores - CNO, Operações Psicológicas, Guerra Eletrónica, Segurança das Operações, Deceção Militar, Information Assurance, Intelligence Surveillance Target Aquisition and Reconaissance - ISTAR, Cooperação Civil-Militar - CIMIC e Informação Pública), permita garantir a coerência do seu planeamento e a execução sincronizada das ações a desenvolver.

- **Um Centro de Ciberdefesa** que permita assegurar a Garantia da Informação (Information Assurance) através da proteção e defesa das Infraestruturas de Informação e da Segurança da Informação do Exército contra eventuais ciberataques (de âmbito nacional ou internacional) que ponham em causa a obtenção da Superioridade de Informação das Forças Terrestres e afetem a Sociedade Portuguesa. O levantamento deste Centro enquadra-se no âmbito de esforços cooperativos já lançados pelas Organizações Internacionais de que Portugal faz parte integrante (OTAN e UE) e por outros Países

1 A Superioridade de Informação ("Information Superiority"), conforme refere o JP 3-13 (2006, p.GL-9), traduz uma situação de vantagem no domínio da informação, resultante da capacidade para "reunir, processar e disseminar um fluxo ininterrupto de informação enquanto se explora ou nega a capacidade de um competidor/adversário poder fazer o mesmo". Uma vez garantida a disponibilidade e a integridade dos Sistemas de Informação, uma opção futura que se coloca é a expansão da influência do seu ambiente de informação (Info-esfera) em direção a outros ambientes mais alargados, dentro dos quais a Organização ou o Estado pretende intervir.



que, de forma individual ou cooperativa, procuram também estruturar uma capacidade neste domínio.

4. A Visão

A "visão para a Superioridade de Informação", clarificadora dos esforços a desenvolver neste domínio, materializa assim a forma como o Exército deverá extrair o valor decorrente de uma utilização cada vez mais coerente, integrada e segura do ambiente de informação. Desenvolve-se a partir de referências doutrinárias aprovadas, garantindo uma convergência para Objetivos de Força Nacionais, definidos tanto no plano interno como no quadro dos compromissos internacionais assumidos por Portugal (OTAN e UE).

De acordo com este enquadramento, os principais elementos resultantes são:

- Uma visão estratégica destinada a garantir a Superioridade de Informação do Exército, estruturada com base na necessidade de definir uma governação (governance) coerente e integrada do ambiente de informação, condição necessária à operação eficiente e eficaz do Sistema de Forças do Exército;

- Um caminho concreto (roadmap) a seguir para a implementação desta visão.

A visão e o roadmap são definidos de forma integrada, sendo o roadmap descrito ao longo de três horizontes temporais, caracterizando a finalidade e os objetivos a atingir no curto (2014), médio (2020) e longo prazo (2030). A visão para atingir a Superioridade de Informação, caracteriza de forma mais detalhada "o que" necessita de ser atingido, ao passo que o roadmap procura recomendar e propor medidas concretas relativamente à forma "como" a visão poderá ser implementada[1] . Ainda que de forma genérica, este tipo de análise pretende clarificar as implicações estruturais, operacionais e genéticas associadas à visão estratégica.

Tendo por base o facto de se prever no curto prazo (até 2014) a implementação de um núcleo de serviços base[2] , destinados a suportar a interação de diferentes comunidades de interesse especializadas, prevê-se já no médio prazo (até 2020) a existência de uma taxonomia de serviços integrada, capaz de permitir levantar um Sistema Integrado de Gestão da Informação do Exército e implementar mecanismos de Controlo de Gestão (Balanced Scorecard). No longo prazo (2030) todos os sistemas tecnológicos utilizados no âmbito da Defesa Nacional terão que operar de acordo com uma arquitetura de informação comum. A interoperabilidade é garantida através da federação de Redes e Sistemas de Informação e surge de forma transparente para os utilizadores, facilitando o desenvolvimento de um Portal de acesso aos vários centros de conhecimento do Exército e estimulando a criação de um Sistema Integrado de Gestão do Conhecimento. Esta transição, quando equacionada em termos estruturais, operacionais e genéticos, consubstancia uma aproximação integrada à mudança, beneficiando e fornecendo orientações para três dimensões-chave: Pessoas (visão estrutural), Informação (visão operacional) e Tecnologia (visão genética). Constituindo a informação um domínio transversal a todas as atividades das Forças Armadas, foi

1 Ao longo das faixas temporais identificadas, procura-se assim caracterizar de forma sequencial o que se procura atingir, estabelecendo-se uma análise multidimensional sob a forma matricial (ex: para dar resposta à questão: O que necessita de ser feito nos vários domínios (estrutural, operacional e genético) para se obter determinada finalidade ou objetivo)

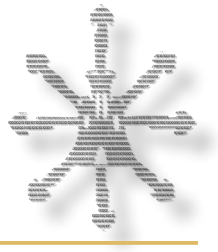
2 Constituindo módulos de um futuro Sistema Integrado de Gestão de Informação, o Exército pretende levantar neste âmbito um Sistema de Gestão Documental (em fase de implementação), um Sistema de Gestão de Tarefas e um Portal Colaborativo.

desenvolvida uma visão de "360º", integrada e coerente do ambiente de informação. O levantamento de uma capacidade de gestão/coordenação de topo do domínio da Informação revela-se assim imprescindível para resolver potenciais problemas e contribuir para a coerência e integração funcional de diversas áreas-chave (e.g.: Controlo de Gestão/Balanced Scorecard, Segurança da Informação, Informações, ISTAR e GE), ligadas tanto ao apoio CSI como à área da Guerra de Informação. A gestão/coordenação destas áreas trará a coerência através da reengenharia de processos e esta, por seu turno, encorajará uma revisão dos processos da organização, analisando a sua conformidade com os objetivos a atingir e avaliando a possibilidade de os adaptar/reformular de acordo com os vetores-chave de desenvolvimento de uma capacidade militar. Em linha com as orientações vertidas na Diretiva Nº02/09 CEME, a decisão de desenvolver novas capacidades no domínio da informação, como o levantamento de um "Elemento de Guerra de Informação" ou de um "Batalhão ISTAR", contribuindo para a obtenção da Superioridade de Informação do Exército, apresenta importantes desafios de natureza doutrinária e genética, obrigando a uma profunda reflexão sobre a sua utilização operacional. Para a concretização desta visão, com uma intervenção determinante das capacidades residentes na Arma de Transmissões, dois outros Órgãos são cruciais: a Academia Militar (AM) – o único Pólo de Investigação e Desenvolvimento que o Exército possui e o Comando da Instrução e Doutrina (CID), a entidade responsável por definir e aprovar o quadro doutrinário de suporte às atividades a desenvolver. A Direção de Comunicações e Sistemas de Informação (DCSI), atualmente na dependência do Comando das Forças Terrestres (CFT), inclui já na sua atividade operacional mecanismos capazes de gerar diversas capacidades no domínio CSI e da Guerra de Informação. Face à especificidade das suas atribuições, a DCSI/CFT poderá assumir naturalmente o papel de Framework Organization no levantamento desta arquitetura que, pela natureza transversal da informação e atendendo ao aumento da sua importância como 5º domínio operacional, obrigará a considerar a possível criação de uma capacidade de Gestão e de condução de Operações de Informação na Estrutura Superior do Exército. A visão proposta, porque permite aproveitar um elevado número de capacidades que o Exército já possui e porque permite perspetivar de forma integrada e proactiva a atuação das Forças Terrestres no ambiente de informação, traça um rumo claro de mudança. Materializando uma alteração do paradigma atual, que contraria uma visão segmentada e uma utilização não coordenada das capacidades existentes neste domínio, a implementação da visão proposta assenta em três objetivos estratégicos estruturantes (ver figura 1):

- Explorar e potenciar a utilização da informação: através da consolidação e integração do apoio CSI;

- Defender e Proteger o ambiente de Informação: através do levantamento de uma Capacidade de Guerra de Informação que permita garantir tanto a disponibilidade e integridade (Information Assurance) como a possibilidade de intervir no domínio da informação de forma concertada (Operações de Informação) no sentido da obtenção da Superioridade de Informação, e,

- Garantir a Gestão de Topo (Governance) do ambiente de Informação: através da coordenação do planeamento e da sincronização de todas as atividades (CSI e de Guerra de Informação) a desenvolver pelo Exército no ambiente de informação, permitindo explorar sinergias e maximizar a utilização dos recursos disponíveis. A "visão para a Superioridade de Informação" materializa assim a forma como o Exército deverá extrair o valor decorrente de uma utilização cada vez mais coerente, integrada e segura do ambiente de informação. Neste contexto, importa salientar nesta visão, de



definição estratégica, os seguintes aspetos:

- Traduz uma arquitetura coerente e lógica, em linha com a dinâmica da envolvente social e com o ambiente operacional em que as Forças Armadas do Século XXI têm que atuar;

- Apresenta um conjunto de objetivos estratégicos bem definidos e realizáveis que, permitindo implementar mecanismos de governação das diversas atividades desenvolvidas pelo Exército no domínio da Informação, contribuirá decisivamente para a sua eficácia operacional;

- É suportada por elementos estruturais e por áreas de conhecimento em relação às quais o Exército já possui uma base de competências;

- Desenvolve-se a partir de conceitos e referências doutrinárias aprovadas, garantindo uma convergência para Objetivos de Força Nacionais[1] , definidos tanto no plano interno como no quadro dos compromissos internacionais assumidos por Portugal (OTAN e UE).

- Prepara o futuro, permitindo ao Exército, na ótica de serviço público, assumir-se como elemento gerador de futuras capacidades de duplo uso Civil-Militar, no quadro do desenvolvimento da Estratégia da Informação Nacional e do levantamento de uma capacidade de Ciberdefesa do País.

- Está de acordo com os eixos de atuação do Plano Global Estratégico de Racionalização e Redução das TIC, na Administração Pública, e as medidas para a consolidação de uma
capacidade de Ciberdefesa do País.

- Está de acordo com os eixos de atuação do Plano Global Estratégico de Racionalização e Redução das TIC, na Administração Pública, e as medidas para a consolidação de uma
Estratégia Nacional para a Segurança da Informação e melhoria dos mecanismos de governabilidade (RCM, 2011: 4848; RCM, 2012: 596).

1 No âmbito das últimas reuniões bilaterais Portugal-NATO (29-30 Nov10), foi identificada como uma das principais lacunas nacionais a inexistência de uma Capacidade Nacional de Ciberdefesa. No caso específico do Exército, estas lacunas traduzem-se em dificuldades identificadas ao nível da adoção dos princípios NEC e da Information Assurance (Ciberdefesa e INFOSEC).



Fig 1 - Visão Integrada do Domínio da Informação

5. O Plano

O Plano de Ação para a Superioridade de Informação seguiu uma metodologia semelhante à utilizada no estudo de implementação da capacidade NEC (Network Enabled Capability) da UE e foi deduzido com base nos requisitos de capacidade definidos pelas suas três dimensões (Pessoas, Informação e Tecnologia), conforme se encontra expresso na visão a atingir. De acordo com a metodologia adotada, este Plano de Ação integra três elementos estruturantes, que se articulam de forma sequencial, garantindo a lógica e a coerência necessárias ao desenvolvimento de uma nova capacidade. Neste contexto, importa identificar os seguintes elementos:

- A Visão – define "o que" se pretende atingir e onde são também identificados os objetivos a atingir ao longo do tempo;

- O Roadmap – onde se clarifica "o como" se atingem os objetivos/metas estabelecidas. Confrontando os objetivos a atingir, com o resultado da análise dos recursos existentes, são identificadas as lacunas existentes. Tendo em vista a edificação plena da Capacidade, o roadmap define assim as condições necessárias à resolução das lacunas identificadas.

- O Plano de Implementação – onde se clarifica "de que forma" se pretendem resolver as lacunas identificadas, ao nível dos diversos vetores de desenvolvimento, e se pretende promover a gestão criteriosa dessas lacunas de forma a implementar a capacidade.

A metodologia adotada, promovendo a gestão das lacunas existentes, serve como matriz orientadora para a elaboração do Plano de Implementação da Capacidade, estabelecendo um conjunto de necessidades-chave a que importa dar resposta ao longo do tempo. Estas necessidades, refletindo-se ao nível dos diversos vetores de desenvolvimento, consubstanciam ações concretas que se revelam absolutamente necessárias para implementar a visão.

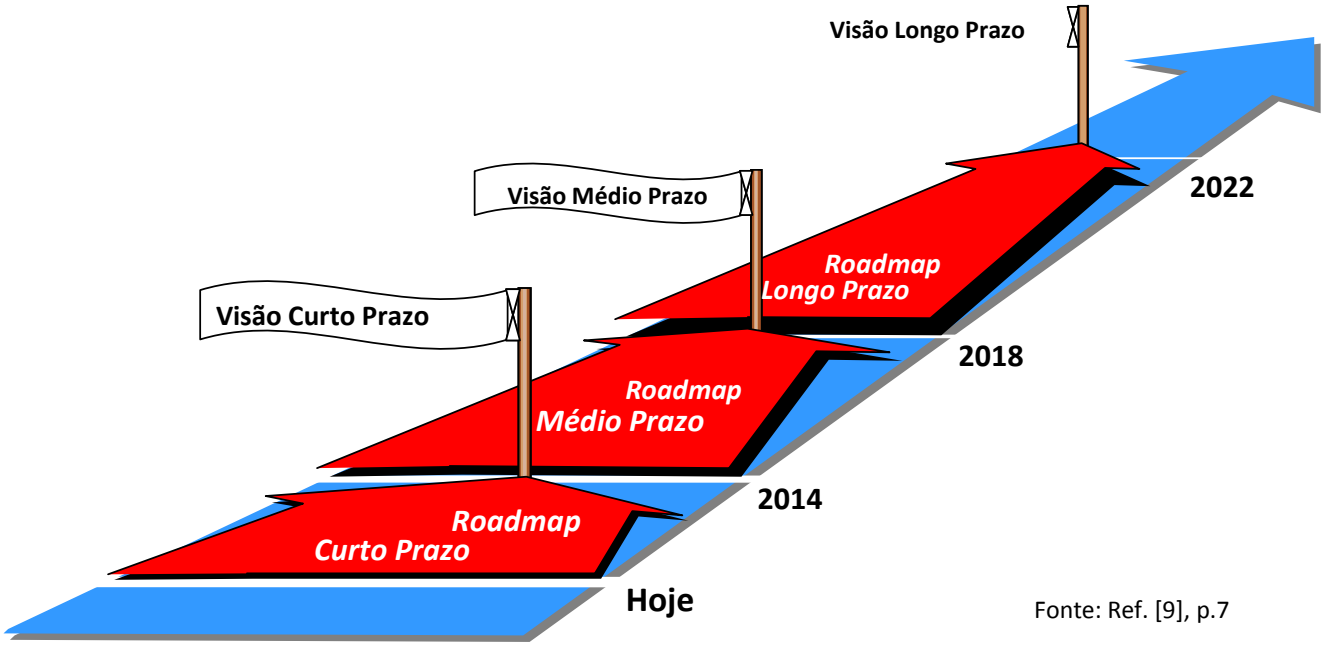


Figura 2: Complementaridade existente entre a Visão e o Roadmap

Podemos afirmar que o Plano de Ação, parte de uma visão estratégica de longo prazo, destinada a garantir a Superioridade de Informação do Exército, e define um caminho concreto (roadmap) a seguir para a sua implementação (ver Figura 2), alinhado e articulado com os Ciclos de Planeamento de Defesa Militar (CPDM) definidos. As três etapas, que marcam este caminho, estão associadas a três metas/objetivos principais a atingir pela visão ao longo dos três primeiros CPDM: curto prazo (até 2014), médio prazo (2014-2018) e longo prazo (2019-2022). Garante-se desta forma, ao longo do tempo, a coerência e a necessária complementaridade entre a visão e o roadmap estabelecido[1] .

Tendo por base a metodologia adotada no âmbito do processo de desenvolvimento de capacidades do Exército e como referência o roadmap antes estabelecido, é então definido um Plano de Implementação. Este fornece uma lista de ações destinadas a garantir a implementação da visão, descrevendo os passos concretos que são necessários dar ao nível dos diversos Vetores de Desenvolvimento desta Capacidade, identificando os atores envolvidos e as suas dependências.

1 Respeitando os CPDM, será possível também harmonizar, articular e otimizar o Planeamento de Defesa Militar Nacional com o ciclo de planeamento NATO e o processo de desenvolvimento de capacidades da UE.

O roadmap associado ao levantamento da Capacidade de Superioridade de Informação resulta da integração de duas aproximações de natureza diferente, refletindo uma orientação do tipo:

- Top-down – que tem por base a visão formulada e os estudos em curso na OTAN e na UE, de forma a determinar um conjunto de elementos-chave necessários à sua implementação.
- Bottom-up – que tem em consideração os Projetos de Implementação já em curso no Exército e que procura, de forma realista, promover a partir daí a sua integração e convergência com outros PIC, a levantar ao longo do tempo, de forma a garantir a edificação das componentes estruturantes desta capacidade;

Confrontando o que é necessário para atingir as metas/objetivos definidos com os recursos existentes, constata-se que existem lacunas que importa resolver de forma a garantir a plena edificação das diversas áreas que permitem garantir a Superioridade de Informação do Exército.

O roadmap contém recomendações e ações concretas a desenvolver, alinhadas e associadas aos três horizontes/metas temporais da visão para a Superioridade de Informação, conforme se encontra representado na Figura 2:

- Curto prazo (até 2014): reformulação de Projetos de Implementação (em curso) e o lançamento de novos PI, incluindo propostas de adoção imediata, destinadas a facilitar o processo de revisão da Lei de Programação Militar (LPM) que se perspetiva venha a ocorrer em 2012. De forma a consolidar o levantamento e a sincronização dos diferentes vetores de capacidade envolvidos, deverão também ser previstas atividades de experimentação e desenvolvimentos de curto prazo, destinados a garantir a sincronização horizontal e vertical dos mesmos.

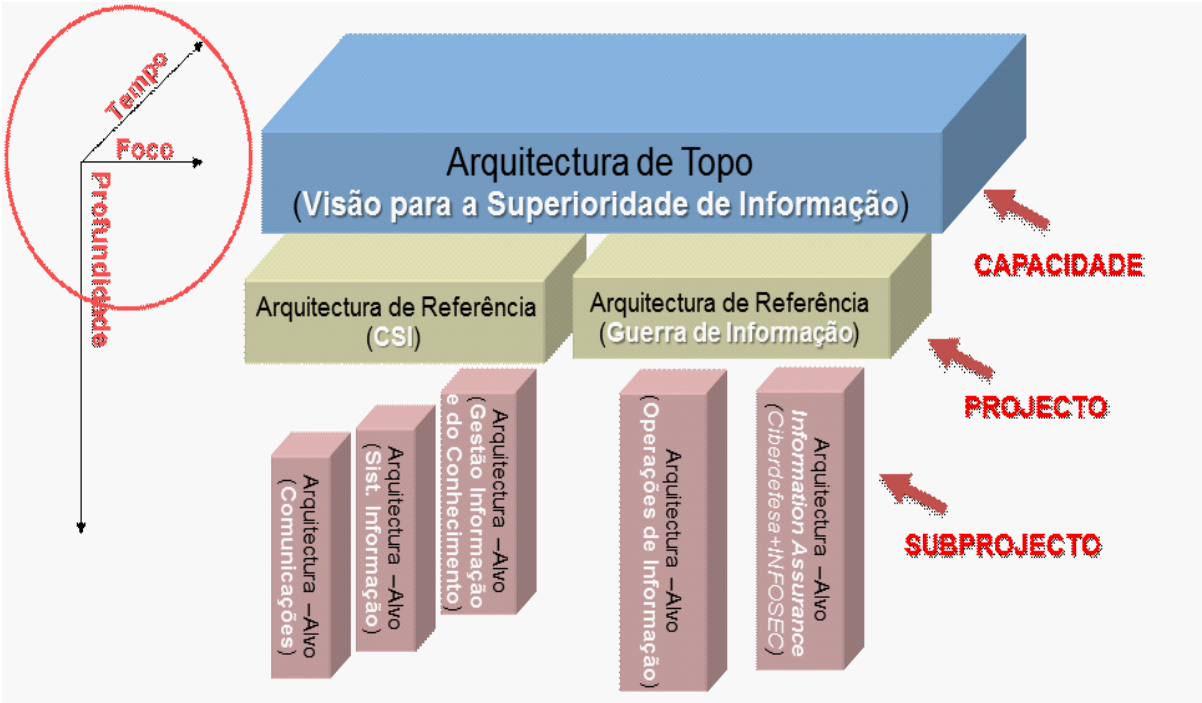


Figura 3 – Federação de Arquiteturas da Capacidade de Superioridade de Informação

- Médio prazo (2014-2018), incluindo a revisão/reformulação dos PI de acordo com uma arquitetura de referência (a definir) e propostas de I&D para investigação e experimentação, demonstração e desenvolvimentos de médio prazo,

- Longo prazo (2019-2022): projetos orientados para a visão de Longo Prazo, promovendo a implementação de arquiteturas-alvo a levantar.

Procurando realizar a ponte entre os Projetos de Implementação (em curso e a levantar) e a edificação plena da Capacidade de Superioridade de Informação do Exército, é definida uma federação de arquiteturas (ver Figura 3).
Tendo por base o enquadramento conceptual e a lógica associada à articulação destas arquiteturas, será possível perspetivar de forma sólida e integrada, o levantamento da capacidade de Superioridade de Informação, conforme se representa na Figura 3. Constituindo a "Visão para a Superioridade de informação" o documento estruturante da nossa arquitetura de topo, é possível reconhecer desde logo a necessidade de definir as duas arquiteturas de referência apresentadas (CSI e Guerra de Informação) e a possibilidade de detalhar as diversas arquiteturas-alvo que permitem edificar cada uma delas. Neste contexto, para a área nuclear do apoio CSI são definidas as seguintes arquiteturas-alvo: Comunicações (Federação de Redes fixas/projetáveis), e Sistemas de Informação (Federação e Gestão de Sistemas de Informação) e Gestão de Informação e do Conhecimento. No âmbito da Guerra de Informação, são também definidas duas arquiteturas-alvo: Information Assurance e Operações de Informação.

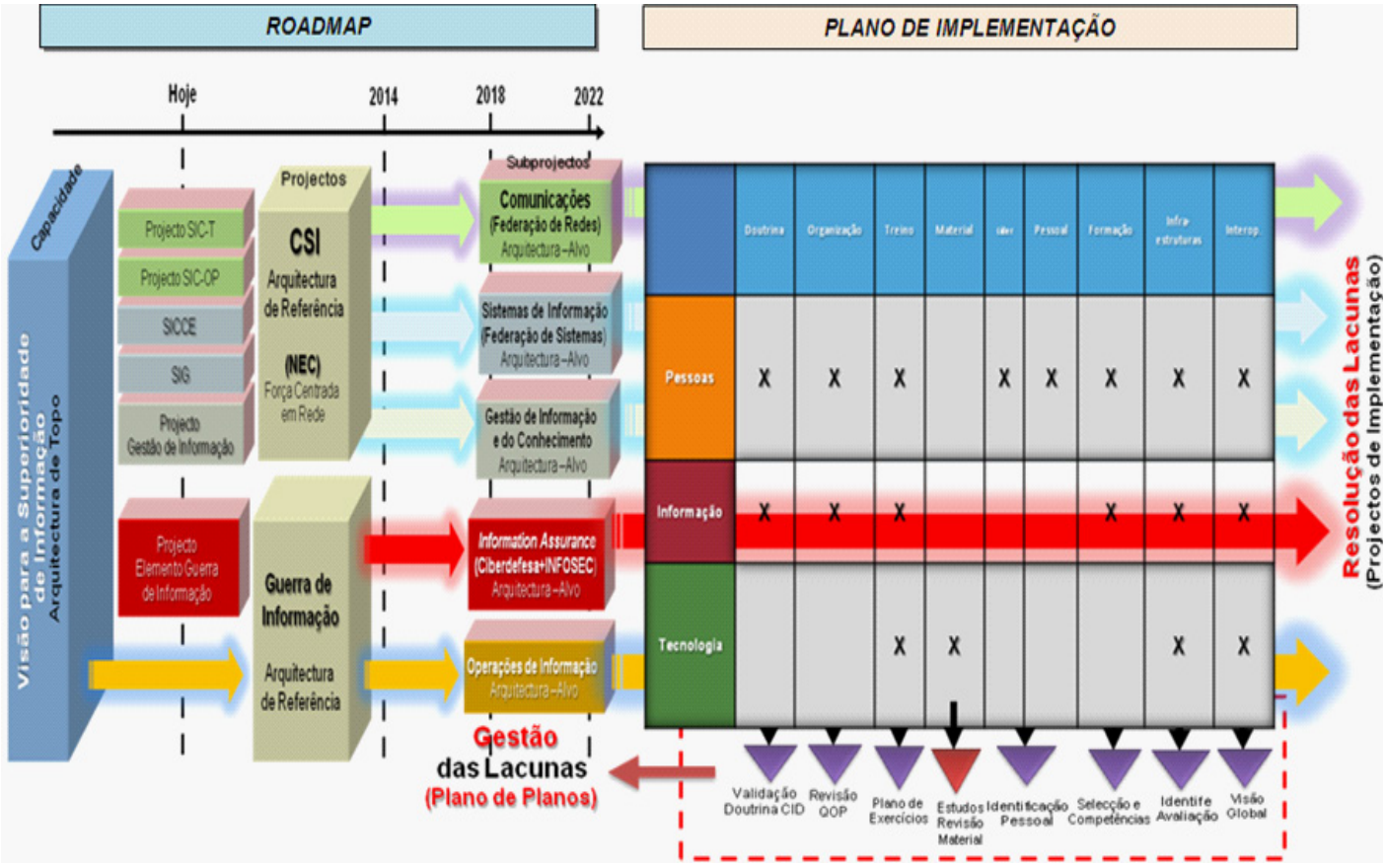


Figura 4 – Roadmap e Plano de Implementação Associados à Capacidade de Superioridade de Informação

Com base no roadmap traçado para o levantamento desta capacidade, importa agora definir para cada um dos Vetores de Desenvolvimento o conjunto de ações que é necessário realizar, garantindo a sincronização de todos os Projetos de Implementação de Capacidade já em curso ou a lançar neste domínio. Conforme se ilustra na figura 4, pretende-se que os vários Projetos e Subprojectos que vierem a surgir, sejam devidamente coordenados e articulados ao longo do tempo.

Sendo lógico assumir que tanto os Projetos como os Subprojectos são levantados para resolver/suprir as lacunas identificadas na edificação da capacidade de Superioridade de Informação do Exército, este Plano de Implementação revela-se essencial para a gestão integrada do processo de resolução das lacunas existentes, garantindo a coerência e a sincronização das ações a desenvolver no âmbito dos diversos Vetores de Desenvolvimento. Na prática, respeitando a especificidade das diversas componentes que permitem edificar uma capacidade, este Plano de Implementação passará pela coordenação de um conjunto de planos sectoriais com foco em cada um dos Vetores de Desenvolvimento, podendo ser perspetivado como um "plano de planos".

6. Vetores de Desenvolvimento Organização e Pessoal

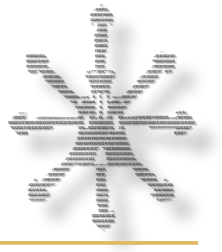
Respeitando a metodologia GPEX e a especificidade das diversas componentes que permitem edificar esta capacidade, o Plano de Ação traçado passa pela coordenação de um conjunto de planos sectoriais com foco em cada um dos Vetores de Desenvolvimento. Assim sendo, é aqui proposto um Plano de Implementação para os vetores "Organização" e "Pessoal" da Capacidade de Superioridade de Informação do Exército. Através da definição de uma Initial Operational Capability- IOC (até 2014) e de uma Full Operational Capability-FOC (até 2022) foram definidas de forma coerente e faseada as necessidades totais de efetivos que, permitindo implementar mecanismos de governação das diversas atividades desenvolvidas pelo Exército no domínio da Informação, contribuirão decisivamente para a sua eficácia operacional.

Face aos constrangimentos existentes, atendendo à extinção dos Oficiais Técnicos de Tm e ao número reduzido de entradas de Oficiais do QP no quadro de Transmissões, registada ao longo dos últimos anos, considera-se necessário um aumento mínimo do número de efetivos da Arma de Transmissões de Oficiais TM401 e Sargentos Tm até 2022 (FOC). Este aumento deve-se essencialmente à criação do Centro de Dados do Exército no RT[1] e à criação do Centro de Ciberdefesa que constituirá uma nova estrutura orgânica. Tendo por base o pressuposto de que todos os ajustamentos necessários devem decorrer dentro do Quadro Legal instituído, a estrutura orgânica para a Superioridade de Informação do Exército foi desenhada com base na possibilidade de colocar na dependência hierárquica direta da DCSI/CFT o Centro de Ciberdefesa e o Centro de Operações de Informação a levantar[2], sem que tal implicasse a necessidade de rever a atual Lei Orgânica do Exército.

---

1 O Centro de dados do Exército pretende colmatar a lacuna existente desde a extinção do CIE, sendo guarnecido com base no pessoal atualmente colocado no Centro de Dados da Defesa, cuja responsabilidade é a de manter as aplicações legadas do Exército.

2 Relativamente à escolha dos modelos orgânicos de referência (NATO e EUA) para estes Centros, a solução levantada pela DivCSI procurou essencialmente recolher os seus princípios doutrinários, enformadores da doutrina de referência nacional. Neste âmbito, realizando uma análise funcional de estruturas afins, no caso do Centro de Ciberdefesa foi analisado o NATO Information Assurance Technical Center (NIATC) e, no caso do Centro de Operações de Informação, o Batalhão de INFO OPS do Exército dos EUA. Neste contexto, atendendo aos Objetivos de Força a atingir, à dimensão do Sistema de Forças do Exército Português e aos constrangimentos de Pessoal existentes, a solução proposta considera-se equilibrada e realista uma vez que, com um efetivo relativamente reduzido, o Exército poderá aumentar a sua eficácia operacional através da produção de efeitos não cinéticos e da condução de ações de Guerra de Informação. A adoção de modelos orgânicos inspirados nos mesmos princípios da NATO e dos EUA permitirá também reduzir o tempo necessário ao levantamento da capacidade, garantindo desta forma uma maior solidez doutrinária, incorporando, sempre que tal se revelar ajustado, procedimentos operacionais e manuais técnicos já consolidados.



Estes dois Centros passariam assim a constituir Unidades de execução no domínio da Guerra de Informação, a par do RT que se manteria como Unidade de Execução para a área CSI. A impossibilidade de criar estes dois Centros como Unidades de execução autónomas, e atendendo ao princípio da separação orgânica entre os níveis de planeamento e execução poderá obrigar, a utilizar Estruturas orgânicas já existentes. Atendendo à orientação seguida, para habilitar a materialização da gestão de topo do domínio da informação, afigura-se necessário proceder à revisão articulada dos QOP das UEO do Exército que contribuem para esta Capacidade. Nomeadamente a revisão dos Quadros Orgânicos da DCSI/CFT, da DivCSI/EME, da EPT e do RT. Considerando que se trata de uma área de relevância operacional crescente e de conhecimento especializado, onde os recursos existentes (humanos e materiais) são reduzidos, espera-se que seja atribuída no curto prazo (até 2014) especial prioridade ao recrutamento de especialistas e ao desenvolvimento das suas competências, recorrendo, sempre que a insuficiência de Oficiais TM401 assim o ditar, a Oficiais de QAS dotados das necessárias qualificações específicas.

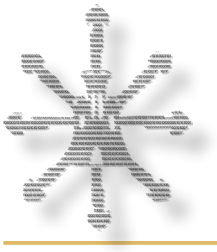
7. Os Próximos Passos

Tratando-se da implementação de uma nova capacidade, a realização de Exercícios e as atividades de Treino Coletivo constituem um fator essencial para a introdução e validação de novas doutrinas e procedimentos operacionais. Neste contexto, assume especial importância a realização de Exercícios periódicos no domínio das Operações de Informação e da Ciberdefesa, equacionados e desenvolvidos, sempre que possível, ao nível do Exército, das Forças Armadas, no plano nacional e internacional.

No âmbito deste vetor de desenvolvimento, considera-se desejável manter uma visão integrada e articulada dos Exercícios e atividades de Treino a desenvolver. Neste domínio, pretende-se implementar um ciclo integrado de Exercícios com a duração de dois anos. Este ciclo contempla a realização de um Exercício de Ciberdefesa (1º Semestre), seguido de um exercício de Operações de Informação (2º Semestre) e de um exercício integrado de Operações de Informação/Ciberdefesa (3º Semestre) onde serão exercitadas todas as componentes da Superioridade de Informação. O 4º Semestre será reservado para a análise das lições aprendidas no âmbito deste ciclo de Exercícios que, entre outros aspetos, poderá vir a contribuir para uma eventual revisão doutrinária e orgânica.

A responsabilidade de coordenação deste ciclo de Exercícios, respeitando a lógica da sua integração na atividade operacional das Forças Terrestres, deverá ser atribuída ao CFT. A DCSI/CFT e a DSCMil/EME assegurarão respetivamente a sua execução e coordenação ao nível da estrutura superior do Exército. A formação e a educação constituem duas áreas nucleares para a geração e desenvolvimento de competências específicas nos recursos humanos que forem selecionados para o desempenho de funções nas diversas estruturas orgânicas, responsáveis pela operacionalização da superioridade de Informação do Exército. Dentro deste enquadramento, torna-se necessário articular o desenvolvimento de competências específicas, nomeadamente na área CSI, das INFO OPS, C2W, CNO e IA, com base em dois vetores principais:

- Formação: explorando uma lógica de formação de formadores (Cursos nacionais e no estrangeiro) num primeiro passo (até 2014) e, num segundo passo (a partir de 2014), massificação da formação especializada a quadros em Centros de Formação/ Escolas Práticas do Exército, especialmente orientados para esse efeito;



- Educação: articulando a formação especializada dos quadros com a sua formação académica em Universidades Nacionais e na Academia Militar (AM). Aproveitando as capacidades residentes na AM, importa desenvolver um esforço tripartido através da:

(1) Introdução das disciplinas de "Guerra de Informação", "Gestão de Informação" e "Gestão do Conhecimento" nos planos de Curso da AM;

(2) Criação de um Mestrado Integrado (2011/2012) para os ex-Licenciados da AM, segundo uma visão de completamento de Créditos para os Oficiais de QAS, composto pela frequência de Seminários associados à Superioridade de Informação";

(3) Ampliação do número de Oficias do Exército que frequentam anualmente o Mestrado em Guerra de Informação.

A responsabilidade de coordenação dos Planos de Formação e dos Planos de Educação deverá ser atribuída respetivamente ao CID e à AM. A DCSI/CFT terá um papel ativo na definição das competências a desenvolver, ajustando-as às necessidades decorrentes da mobilização de competências associada à operacionalização das novas capacidades a levantar. A DRec/EME garante a articulação e coordenação destes planos ao nível da Estrutura Superior do Exército.

Conclusão

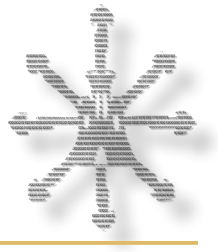
Com a crescente importância das Tecnologias da Informação e Comunicação (TIC) em todas as esferas da sociedade, e naturalmente na Segurança e Defesa Nacional, a questão da Cibersegurança e da Ciberdefesa assumiram assim uma dimensão estratégica. Torna-se assim imperativa a definição de uma Estratégia Nacional de Cibersegurança e Ciberdefesa.

Respeitando as responsabilidades específicas de cada ator, importa assim equacionar o levantamento de um novo e adequado quadro legal, orientado essencialmente para o potenciar de esforços cooperativos e para o desenvolvimento de capacidades de duplo-uso.
O levantamento de um sistema de Ciberdefesa nacional, capaz de fornecer o alerta precoce, de permitir a rápida recuperação e fazer face à ocorrência de ciberataques assume um papel determinante para a proteção das infraestruturas críticas nacionais.
Impõe-se assim desenvolver um esforço concertado tanto na área da Ciberdefesa do País, capaz de explorar sinergias nacionais e estimular a cooperação internacional nestes domínios.

O caminho definido pelo Exército, porque aproveita um elevado número de capacidades residentes, porque permite perspetivar de forma integrada e proactiva a atuação das Forças Terrestres no ambiente de Informação e porque se desenvolve a partir de referências doutrinárias aprovadas, garantindo uma convergência para Objetivos de Força Nacionais, definidos tanto no plano interno como no quadro dos compromissos internacionais assumidos por Portugal, traça um rumo para a obtenção da Superioridade de Informação, "construindo a ponte" com um futuro que importa edificar.

Para fazer face aos desafios que se colocam na Era da Informação, constata-se que o Exército terá que intensificar o esforço de geração de recursos humanos especializados na área das TIC.

Neste âmbito, considera-se que deverá ser mantido ou mesmo incrementado o atual número de admissões à AM e à ESE, configurando-se este como um caminho crítico a seguir para fazer face às solicitações de recursos humanos qualificados que a Superioridade de Informação exige.
Face aos diferentes cenários prospetivos que se colocam ao emprego operacional das Forças Arma-

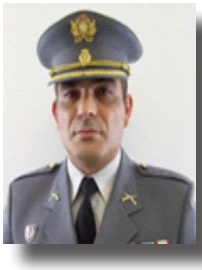


das em geral e das Forças Terrestres em particular, claramente desafiadores e com especiais exigências nas áreas do conhecimento e das novas tecnologias, faz todo o sentido adotar uma visão global (holística) do ambiente de informação em vez de uma perspetiva fragmentada, procurando desenvolver, sempre que possível, uma atitude proactiva em vez de reativa.

Torna-se imperioso dotar o Exército de uma ordenação "urbanística" que preserve e fortaleça a sua posição dentro da sociedade portuguesa. E que inove e acrescente valor ao Estado atual, dotando-o, por via da constituição, de instrumentos novos que capacitem uma melhor atuação sistémica, orquestrando mais eficazmente os seus recursos humanos e materiais, produzindo mais e melhor valor para a Nação.

Como corolário, reforça-se a ideia-força de que esta arquitetura, tão ambiciosa como mobilizadora, cujo objetivo final é conseguir alcançar ganhos de poupança e de eficiência, está claramente ao nosso alcance. A questão a que importa agora dar resposta é a de saber se vamos ser capazes de "fazer a ponte" com o futuro e de a concretizar.

Gestão da Informação no Exército



TCor Inf Mário Pereira

Introdução

A complexidade e o dinamismo que caracteriza o mundo neste início do século XXI, geram um clima de incerteza e de difícil previsibilidade, suscitando a necessidade de melhor informação, em tempo útil, de forma a possibilitar uma tomada de decisão adequada e oportuna.
Esta realidade conduz à necessidade de se encarar a informação como uma atividade vital, constituindo a corrente sanguínea de qualquer organização. Reconhecer esta realidade, e dispor de mecanismos que possibilitem uma gestão efetiva e eficiente de todo o ciclo de vida da informação, incrementa significativamente as possibilidades de sucesso de uma organização comparativamente a outras menos estruturadas neste domínio.
Este conceito em si mesmo, não apresenta propriamente um carácter inovador. Ao longo da história da humanidade, a obtenção de informação precisa, relevante e em tempo oportuno, tem constituído a chave que materializa o sucesso ou o fracasso de muitos empreendimentos, militares, políticos ou de qualquer outra natureza.
Não deixa igualmente de ser verdade, que nos dias de hoje, tal como no passado, embora se reconheça e constate a importância da informação, os esforços nesta área tendem a focar-se nas tecnologias de informação (TI) uma vez que estas são reais, tangíveis e com capacidades em rápido crescimento. A implementação de mecanismos efetivos de gestão do recurso informação que permitam transformar a sua natureza intrinsecamente intangível, assume um carácter decisivo e materializa uma alteração de paradigma.

O Exército e o Ambiente da Informação

Atento a esta realidade, e em alinhamento com as principais organizações internacionais em que Portugal se insere (OTAN e UE), o Exército estabeleceu o objetivo de traçar um caminho que possibilite a sua estruturação para esta nova realidade. No documento "Superioridade de Informação: Um Objetivo Estratégico para o Exército", é materializada a visão do Exército acerca desta matéria, e são delineadas linhas gerais de ação para a coordenação, planeamento e sincronização de todas as atividades a desenvolver pelo Exército no ambiente de informação, de forma a permitir explorar sinergias e maximizar a utilização dos recursos disponíveis.
Partilha rápida da informação, ambientes de rede dinâmicos e facilmente reconfiguráveis, são eleitos como princípios a seguir e objectivos a alcançar. O apoio em Comunicações e Sistemas de Informação (CSI), deve ser equacionado e perspetivado do curto ao longo prazo, e encarado como um programa que suporte a transição para o novo paradigma, possibilitando a implementação de uma gestão coerente e integrada do ambiente de informação do Exército. Desta forma, perspetiva-se a evolução do apoio CSI no Exército Português no sentido de uma federação de Redes e Sistemas de Informação, segundo uma lógica de desenvolvimento de Capacidades Centradas em Rede, respeitando os princípios seguidos pela arquitetura adotada pela OTAN (NATO Network Enabled Capability – NNEC).
Esta visão possibilita e facilita a implementação da metodologia Balanced Scorecard no Exército na medida em que permitirá:
- Dispor de informação sintética e agregada que facilite a gestão estratégica da Organização;
- Maior facilidade na gestão da informação, permitindo obter uma visão equidistante entre a componente operacional e a componente de gestão, esta mais vocacionada para a sustentação logística e administrativa;
- Maior flexibilidade para desenvolver uma arquitetura de informação integrada, facilitan

do o levantamento de mecanismos para a sua proteção e segurança de forma global que, estendendo-se desde o campo de batalha à Estrutura Superior do Exército, permita obter a visibilidade dos processos e a transparência necessária para perceber o impacto de potenciais ataques aos Sistemas de Comando e Controlo (C2).

A Gestão de Informação no EME

A missão atribuída à Divisão de Comunicações e Sistemas de Informação do Estado-Maior do Exército (DivCSI/EME), de criar e gerir um Sistema de Gestão de Informação (SGI) no Estado-Maior do Exército (EME) que permitisse, posteriormente, a sua replicação nos Órgãos Centrais de Administração e Direção (OCAD) e Comando das Forças Terrestres (CFT), insere-se na meta traçada de melhorar a gestão de informação no Exército. O SGI-EME, tem como objetivo a satisfação das necessidades de tratamento de conteúdos, registos e "workflows"[1] nos circuitos documentais, respeitar o ciclo de vida completo [2] dos documentos, ser capaz de suportar o desenvolvimento de mecanismos de controlo de gestão (ex: Balanced Scorecard) em apoio à tomada de decisão em todos os escalões de Comando e garantir a coordenação e sincronização das atividades do Exército. Numa perspetiva de otimização dos recursos existentes foram identificadas três áreas-chave a desenvolver:

- Implementação e/ou desenvolvimento de Portais Colaborativos[3] ;

- Implementação de um sistema de Gestão Documental;

- Implementação de um sistema de Gestão de Tarefas.

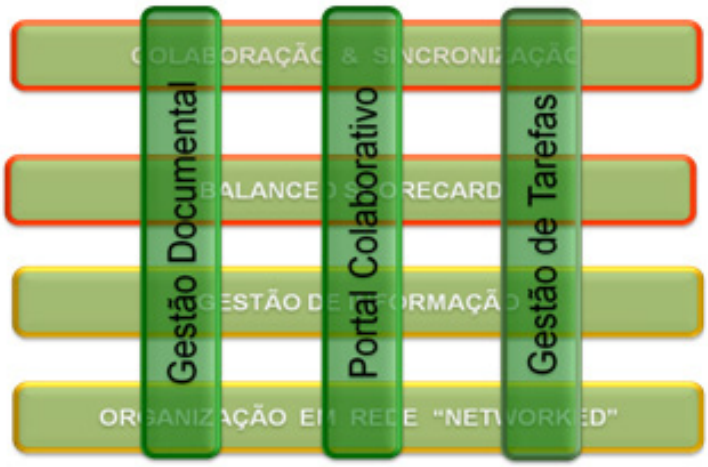


Fig. 1 – Gestão de Informação no EME

1 Recursos de colaboração integrados, como fluxos de trabalho automatizados, que ajudam os utilizadores a trabalhar melhor em conjunto para criar, revisar e aprovar documentos de uma maneira mais estruturada.

2 Entende-se por ciclo de vida, neste contexto específico, criar/capturar, armazenar/gerir, distribuir/partilhar (acesso aos conteúdos através de diferentes canais de comunicação Web ou acesso aos conteúdos através de aplicações específicas da organização) e finalmente preservar/disponibilizar, e assim sucessivamente.

3 Os Portais Colaborativos/Corporativos são ambientes de trabalho integrados, sustentados por TIC, e que proporcionam um ponto único de integração e navegação pela informação e conhecimento, tornando-se o local de trabalho de todos os elementos da organização, permitindo a colaboração, partilha e acesso integrado a toda e qualquer informação que ajude os colaboradores a melhor desempenharem as suas funções na organização.

No seguimento da remodelação do portal da Intranet do Exército por parte do Regimento de Transmissões (passando este a operar com base no Microsoft Office
SharePoint Server 2007), o EME implementou no inicio de 2010, o seu Portal Colaborativo que funciona numa plataforma de Windows SharePoint Services (WSS).

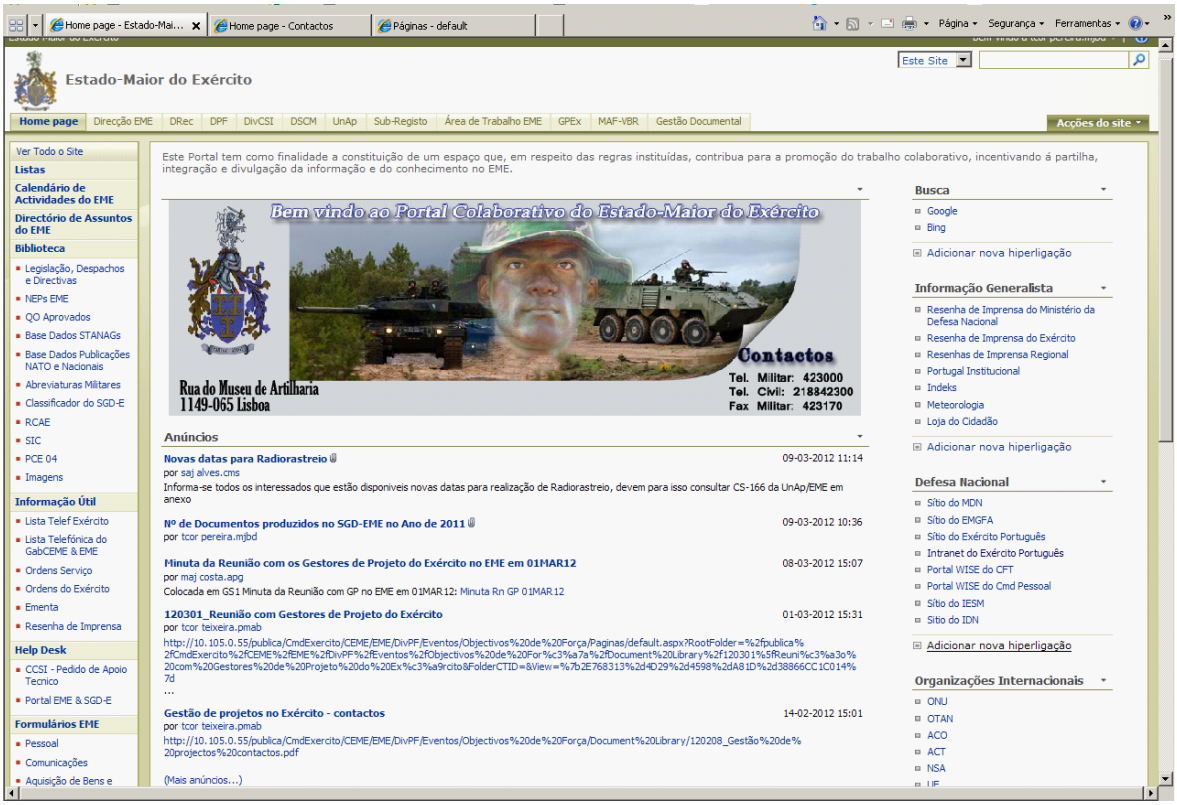


Fig. 2 – Página Principal do Portal Colaborativo do EME

Tendo por pano de fundo, as restrições orçamentais que o País em geral, e o Exército em particular, enfrentam, tornou-se necessário rever e priorizar as ações em curso e a desenvolver no futuro próximo, pelo que se entendeu suspender o processo com vista à aquisição de um sistema de gestão de tarefas[1] , procurando-se colmatar esta necessidade através da exploração das ferramentas já disponíveis (Portal Colaborativo e MS Outlook) em conjugação com um Sistema de Gestão Documental.
Relativamente a este último, e uma vez que o Exército apenas dispunha de uma aplicação de gestão de correspondência, cujo desenvolvimento e suporte tinha sido descontinuado em meados de 2010, foi efetuada uma pesquisa no mercado no sentido de se adquirir uma aplicação COTS[2] para sua substituição, que permitisse centralizar e gerir de uma forma eficiente o ciclo de vida completo de todas as formas de

1 Foi considerada a aquisição da ferramenta "Tasker Tracker", desenvolvida pela Agência NC3A/OTAN. O "Tasker Tracker" permite o desenvolvimento de tarefas num ambiente colaborativo de Estado-Maior (EM), através da automatização de processos, reduzindo, não só, o recurso "tempo", mas também a duplicação de informação e diminuição de e-mail trocado entre os vários participantes de uma tarefa.

2 Commercial of-the-shelf.

conteúdos “estruturados” e “não estruturados”[1] da Organização, e que apresentasse o mínimo possível de necessidades de personalização.
De entre as várias soluções analisadas, considerou-se que a solução adotada é a que mais se ajusta aos requisitos levantados pelo Exército, tendo a sua otimização sido iniciada em finais de 2010 e decorrido ao longo do ano de 2011. Dadas as especificidades da natureza, estrutura e forma de operar do Exército, foi acordado a constituição de duas configurações distintas do Sistema de Gestão Documental – Exército (SGD-E): uma destinada ao EME e OCAD´s; e uma outra para utilização no Gabinete do Chefe de Estado-Maior (Gab CEME) e restantes Unidades, Estabelecimentos e Órgãos do Exército, sendo que os módulos piloto foram instalados no EME e no Regimento de Transmissões (RT), respetivamente.

Sistema de Gestão Documental do Exército (SGD-E)

A solução desenvolvida, apoiando-se numa moderna plataforma tecnológica[2] , proporciona uma eficaz gestão dos fluxos informacionais de uma U/E/O do Exército.

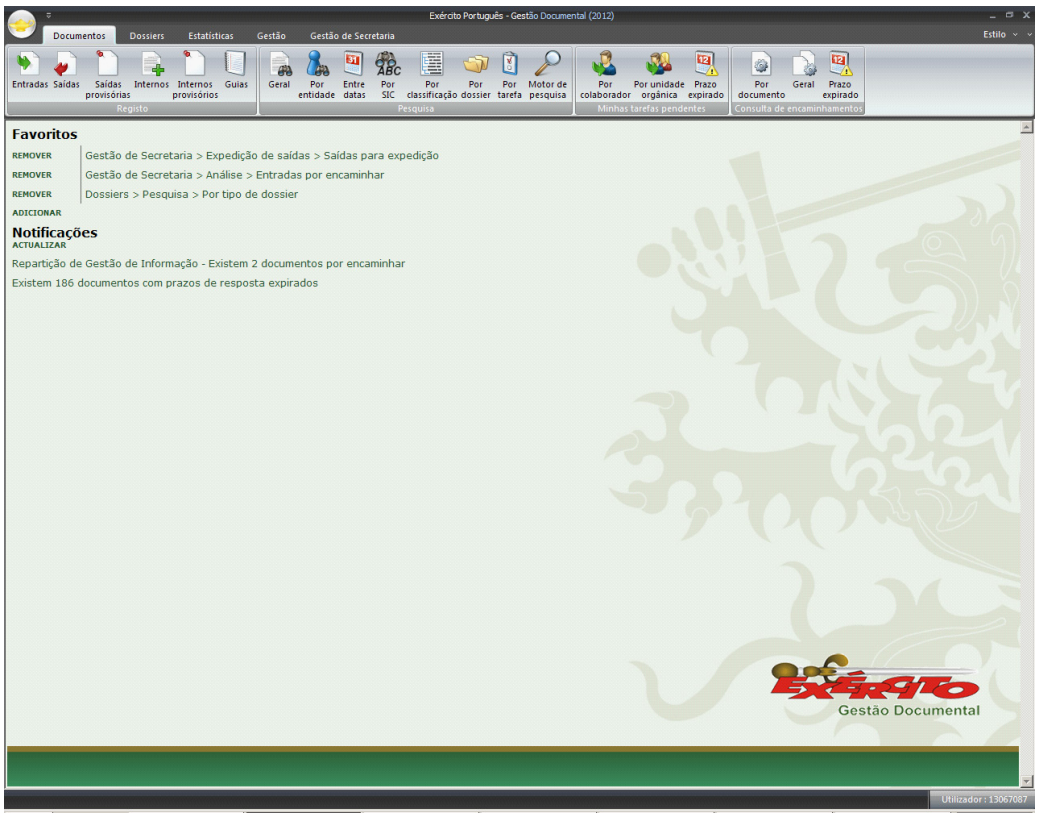


Fig. 3 – Imagem do Interface do SGD-E

1 Por oposição aos conteúdos estruturados que se caracterizam por terem formatos uniformes, serem armazenados centralmente, categorizados para pesquisa e acessíveis a todos os utilizadores.

2 SINGAP - Sistema Integrado para a Nova Gestão da Administração Pública

O SGD-E engloba e responde a um conjunto de funcionalidades, tais como:

- Registo e classificação de entradas e saídas de documentos por vários utilizadores; Os documentos são registados e descritos de acordo com 3 tipos principais, entradas do exterior; saídas para o exterior; documentos produzidos e encaminhados internamente. Qualquer um destes tipos de documentos pode ser inicialmente registado em formato provisório (Draft) e depois ser convertido num documento definitivo através da atribuição de número e data de registo.

- Gestão de encaminhamentos de documentos entre subunidades orgânicas de uma U/E/O; O sistema permite simultaneamente o encaminhamento ad-hoc (manual) ou através de um workflow (circuito pré-configurado). Em qualquer uma destas opções podem ser encaminhados tanto documentos simples como dossiês digitais. O motor de workflows pode ser configurado e alterado autonomamente pelo gestor do sistema. O SGD-E, possibilita ainda o efetuar do acompanhamento de um documento em todo o seu circuito (seja num workflow ou num encaminhamentos ad-hoc).

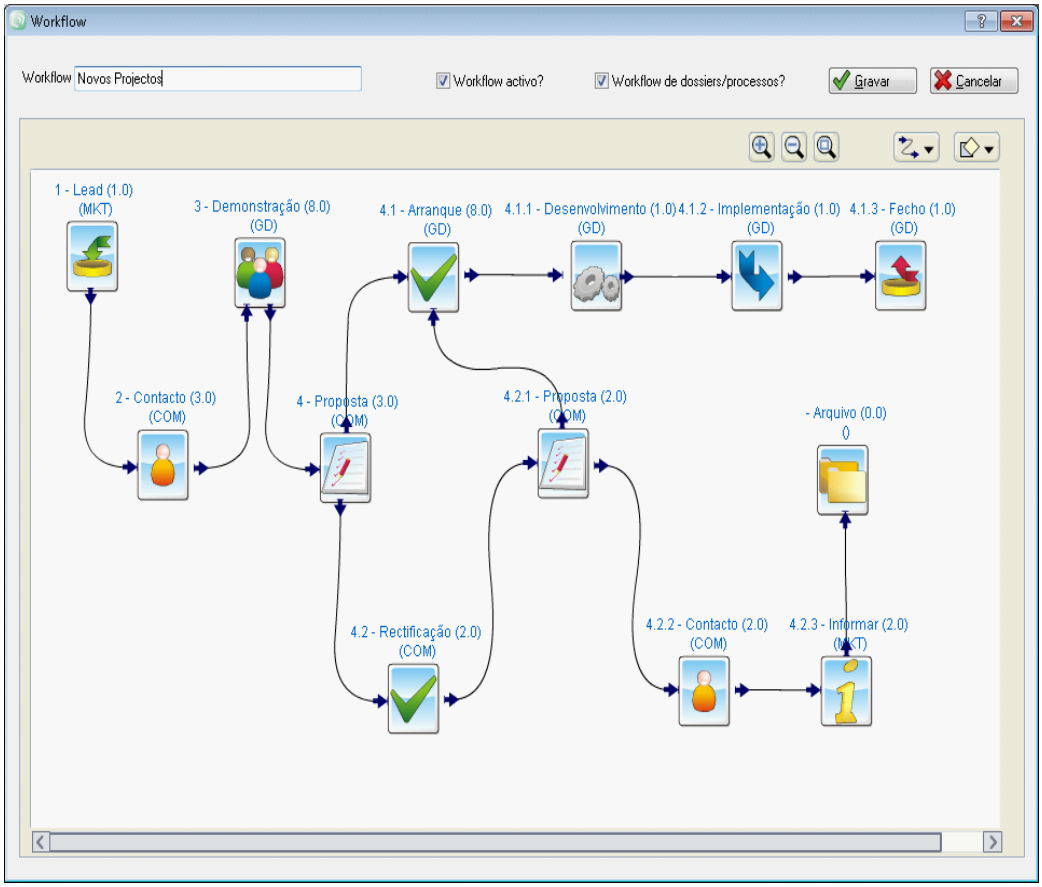
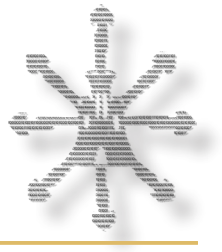


Fig. 4 – Exemplo de um Worflow (SGD-E)



- Assinatura eletrónica de despachos e de documentos com recurso a certificados eletrónicos; A desmaterialização implica que seja necessário assinar digitalmente[1] os documentos e os despachos produzidos no sistema, sendo que este objetivo é cumprido através da utilização de certificados eletrónicos.
Importa aqui referir, que a adoção dos mecanismos exclusivos para a identificação, autenticação e assinatura eletrónica de cidadãos perante entidades do sector público, nomeadamente através do Cartão de Cidadão é obrigatória, tal como expresso na Resolução de Conselho de Ministros nº109/2009, de 2 de Outubro, tendo já decorrido o período transitório de dois anos, no qual outros mecanismos coexistiram.
O Exército estabeleceu contato com a Agência para a Modernização Administrativa (AMA) no sentido de testar a utilização do Certificado Eletrónico do Cartão do Cidadão no SGD-E. Atualmente, por determinação do Chefe de Estado-Maior do Exército, é utilizado o Certificado Eletrónico emitido pelo Centro de Segurança da Informação do RT[2] que constitui a Autoridade Certificadora do Exército, para possibilitar a assinatura de documentos eletrónicos produzidos no SGD-E e expedidos para o seio do Exército. Uma vez que a Autoridade Certificadora do Exército, não é uma entidade certificadora credenciada no âmbito do Sistema de Certificação Eletrónica do Estado, as assinaturas geradas com base nos certificados por ela emitidos, não se constituem em assinaturas eletrónicas qualificadas[3] pelo que na correspondência com entidades exteriores é utilizada a assinatura autografa.

O SGD-E possibilita também a utilização de Certificados Eletrónicos, para autenticação no sistema em substituição da introdução do login e password do utilizador.

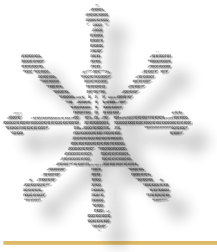
- Organização da informação em processos, agrupando registos de entradas, saídas e documentos internos em conjuntos coerentes de informação.
O sistema de classificação do SGD-E articula-se em 03 níveis:

- 1º Nível – Códigos de Classificação
Constituído pelos códigos de classificação estabelecidos na Portaria 272/2000, de 22 de Maio, Regulamento de Conservação Arquivística do Exército (RCAE); é constituído por uma série de 5 algarismos. Exemplo, 00.060, Assuntos NATO;

1 Assinatura Digital - modalidade de assinatura eletrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento eletrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento eletrónico foi alterado depois de aposta a assinatura (DL 62/2003, Art. 2º, al. d)

2 Na Diretiva 156/CEME/09 é determinado que compete ao Comando Operacional, através do Centro de Segurança da Informação do Regimento de Transmissões, o estabelecimento de uma hierarquia de confiança, com uma Entidade Certificadora do "universo" Exército sediada nesse centro (…)".

3 Assinatura eletrónica qualificada - assinatura digital ou outra modalidade de assinatura eletrónica avançada que satisfaça exigências de segurança idênticas às da assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura (idem, al. g)



- 2º Nível – Dossiê

Combina com o 1º nível, é constituído por uma serie de 4 algarismos que traduzem os "grandes assuntos" do Exército. Exemplo, 4002, Carro de Combate Leopard 2A6;
Relativamente ao termo dossiê, este foi adotado devido ao facto de o sistema permitir a organização de documentos em pastas (dossiês) digitais, bem como o seu encaminhamento. A classificação atribuída ao dossiê é automaticamente replicada para todos os documentos que lhe são associados e a criação de dossiês é automática, mediante o preenchimento do código de classificação (RCAE) e do tipo de dossiê. Assim, reportando-nos ao presente exemplo, o dossiê Carro de Combate (4002), deverá conter a maioria dos documentos relacionados com este assunto; o RCAE é utilizado como o separador dentro do dossiê digital, ou seja, subdivide o grande assunto em áreas parcelares (comando, pessoal, transmissões etc.);

- 3º Nível – Identificação da Unidade Orgânica que elaborou o registo

Combina com os restantes níveis e é constituído por um conjunto parametrizável de 2 algarismos, que identificam quem elaborou o registo do documento; Exemplo, 10, Repartição de Gestão da Informação;
Interpretando a classificação acima descrita, o documento apresentaria o processo 00.060.4002.10, que significa que o assunto principal será o Carro de Combate Leopard 2A6, relacionado com informação ligada à NATO e que foi elaborado pela Repartição de Gestão da Informação. Esta forma de classificação tem dois grandes objetivos: cumprir a legislação em vigor; e evitar a multiplicação de classificadores no seio das U/E/O, com a consequente duplicação de documentos, na medida em que, sempre que exista mais que um classificador e sempre que um documento se destine a mais que uma unidade orgânica interna, terá que ser classificado de forma diferente, resultando que em muitas situações existem duas ou mais cópias do mesmo documento, diferindo estas apenas na sua classificação.

- Geração de documentos no sistema, nomeadamente através da utilização de templates; Os documentos podem ser criados automaticamente através de templates integrados no sistema pelos utilizadores ou pelo gestor do sistema.

- Pesquisa de documentos por critérios múltiplos, como: palavras-chave, remetente/destinatário, data, tipo de documento, origem, entre outros; A pesquisa pode ser efetuada na informação associada a cada ficheiro ou no documento anexo e pode ser filtrada de múltiplas formas. O sistema dispõe ainda, de um motor de pesquisa que permite a recuperação de informação através de uma pesquisa cruzada no conteúdo e nos dados associados a cada documento ou registo.

- Importação e exportação de informação, produção de listagens de histórico ou estatísticas; É possível a exportação da informação em diversos formatos, nomeadamente .csv, .xls e .pdf, bem como, pré-visualizar e imprimir relatórios com dados que podem consistir em listagens de documentos organizadas em função de determinado filtro (ex: produção de registos por Unidade Orgânica etc.). De igual forma, podem ser produzidos relatórios estatísticos elaborados a partir de informação recolhida ao longo do circuito documental (ex: média de duração do circuito). A exportação pode ser efetuada a partir de qualquer listagem do sistema e reflete apenas os dados a que cada utilizador tem acesso, assim como, quaisquer outros filtros que tenham sido aplicados. No que à importação de ficheiros ou documentos diz respeito, estes podem ser importados individualmente ou em grupo, são gravados em formato protegido, permitindo no entanto a criação/gestão de versões dos documentos. A um registo criado no SGD-E pode ser anexado qualquer formato/tipo de ficheiro.

- Gestão de ausências; É disponibilizado um mecanismo de gestão de ausências que redistribui automaticamente o expediente encaminhado para um utilizador ausente para outro indicado pelo próprio para o substituir.

- Gestão da informação em rede; O controlo do acesso à informação (metadados e documentos) é garantido não só através da utilização de perfis de acesso, mas também mediante a estratificação da informação em níveis de confidencialidade (de acordo com o SEGMIL). As alterações à informação são igualmente controladas de forma a possibilitar, por um lado, que por omissão todos os documentos estejam protegidos, e por outro, seja conservado um histórico de todas as suas versões.

- Múltiplos Interfaces;

- Além do interface de produção, o SGD-E dispõe ainda de uma versão Web destinada principalmente a "light users", que pode ser integrada com o portal da organização ou com um gestor de conteúdos como o MS SharePoint. Existem dois tipos de interfaces deste tipo; um com auto-login que utiliza os dados de acesso do utilizador à Rede de Dados do Exército; e um outro que exige a autenticação do utilizador sempre que acede ao sistema.

- Uma vez que o correio eletrónico constitui uma componente cada vez mais significativa do expediente das U/E/O, o sistema dispõe de um interface de integração com o MS Outlook, que permite não só a inclusão no SGD-E dos emails recebidos, como também a expedição por essa via, de documentos eletrónicos produzidos no sistema (sem quebra da assinatura se o documento estiver assinado eletronicamente).

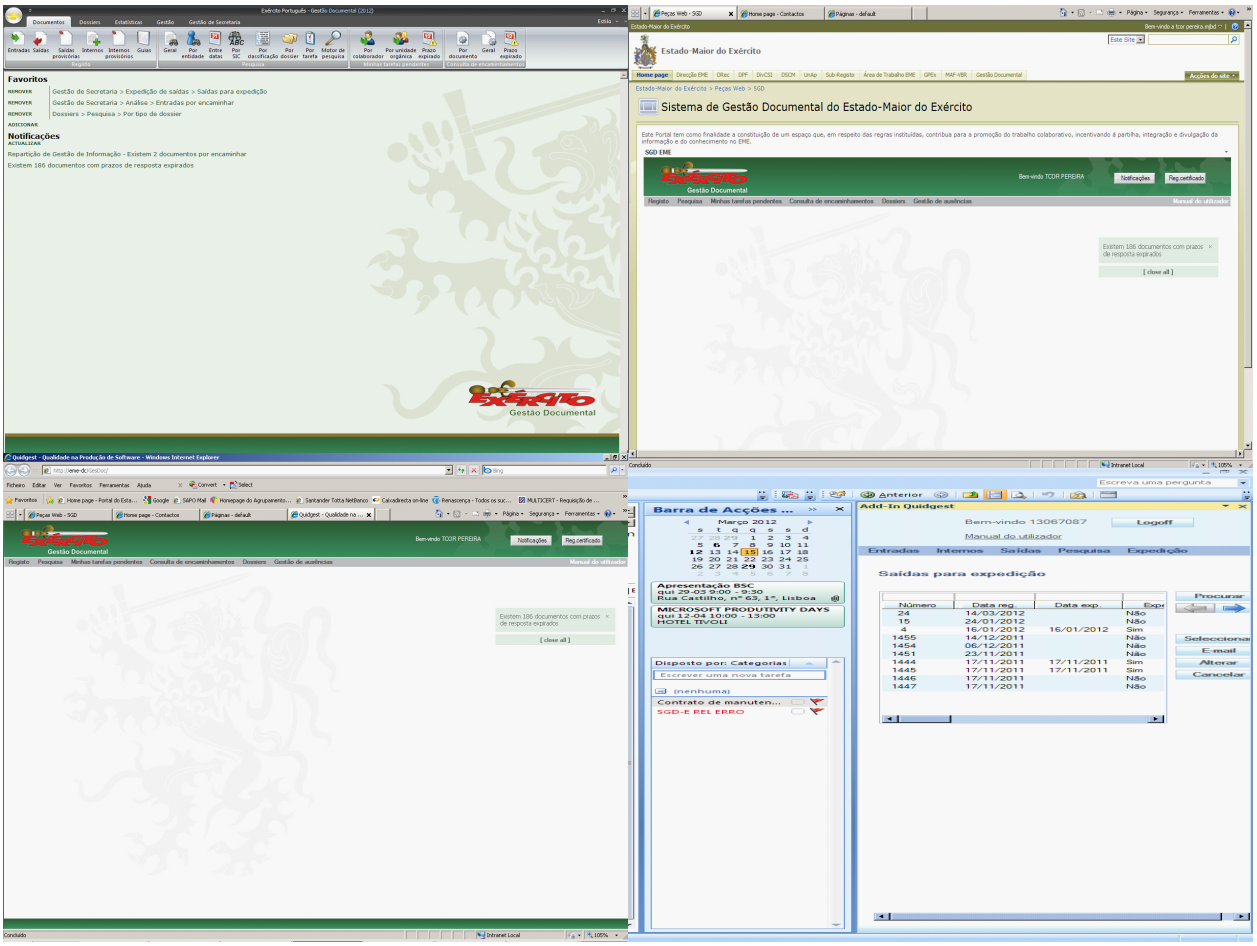


Fig. 5 – Interfaces Disponíveis no SGD-E

Por último, importa referir que as tecnologias utilizadas no SGD-E asseguram a possibilidade do sistema acompanhar o crescimento da organização, sem que isso implique uma perda na sua performance, uma vez que é utilizado um motor de geração automática de código que permite que todos os desenvolvimentos necessários para a evolução conjunta da organização e do sistema, sejam produzidos de forma rápida e homogénea. Realça-se também, que na construção do SGD-E foram considerados os diversos requisitos constantes no modelo MoReq2[1] , a incorporação de thesaurus é efetuada de acordo com as indicações da norma NP4036[2] e a utilização dos diferentes interfaces responde aos requisitos das normas ISAD(G)[3] e ISAAR(CPF)[4] .

Conclusões

Numa época marcada por objetivos da excelência, onde conceitos como rapidez, eficácia, gestão rigorosa de recursos, redução dos custos são indispensáveis para o sucesso das organizações, estes objetivos só podem ser materializados através da introdução de mecanismos de automatização e/ou da (re)engenharia de processos de otimização dos fluxos de informação, mediante o seu tratamento e gestão, criando espaços únicos de trabalho, tornando possível a sua partilha, bem como, estabelecendo canais privilegiados de comunicação, quer com entidades exteriores à organização, quer com os próprios elementos que a integram.
Se no caso do mundo empresarial o risco inerente ao não cumprimento destas premissas, será o de perda de vantagem competitiva ou de falência, no caso das organizações militares o que está em causa pode significar a diferença entre o cumprimento da missão ou o seu incumprimento, com o inerente risco, no limite, de perda de vidas humanas.
Relativamente ao SGD-E, as funcionalidades disponíveis de assinatura eletrónica, gestão de todo o ciclo de vida ativa de um documento, elaboração, validação, seguimento e consulta de despachos, conjugadas com a capacidade já existente no Exército de encriptação e assinatura de correio eletrónico (mediante a utilização de um certificado eletrónico), resulta numa significativa melhoria na rapidez, gestão e controlo dos seus circuitos documentais, possibilita a sua desmaterialização, e representa uma importante e significativa redução dos custos inerentes ao manuseamento, expedição e arquivo de documentos e processos, constituindo um importante contributo para a eficiência do modelo de gestão da informação do Exército.

1 Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos publicado em 2008 pela Comissão Europeia

2 Tesauros monolingues: Diretivas para a construção e desenvolvimento de documentação

3 Norma geral internacional de descrição arquivística

4 Norma Internacional de Registo de Autoridade Arquivística para Pessoas Coletivas, Pessoas Singulares e Famílias

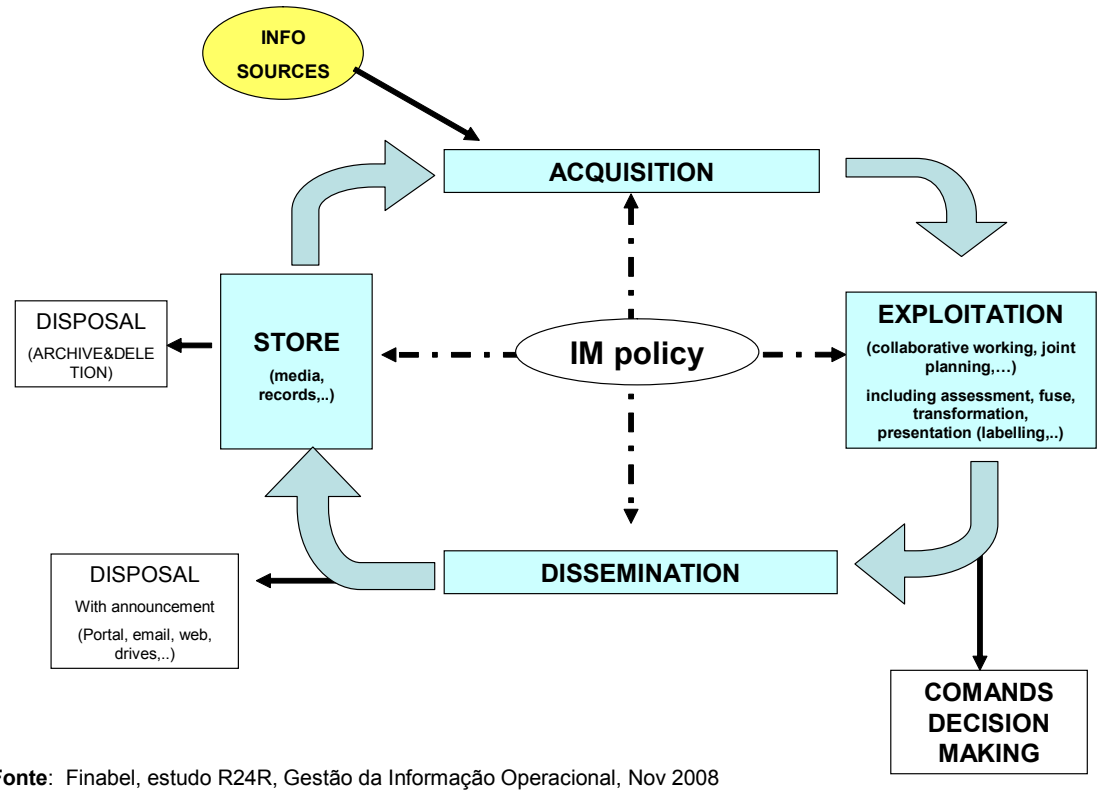
GESTÃO DA INFORMAÇÃO



COR TM (ENG.) ANTONINO MELO

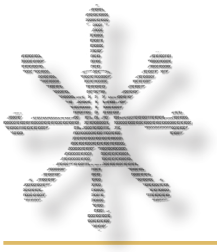
Numa organização em rede e "digitalizada", cujo ambiente se caracteriza pela conectividade perfeita entre todas as entidades e pela universalidade na partilha e acesso à informação, a Gestão da Informação torna-se um importante desafio.

A par da capacidade de aquisição da informação e da sua utilização para criar conhecimento, torna-se fundamental a forma pela qual a organização incorpora nos seus processos internos as facilidades proporcionadas pelas novas tecnologias de
Informação, pois é essa capacidade que contribui para a optimização dos recursos e potencia a criação de valor.



Fonte: Finabel, estudo R24R, Gestão da Informação Operacional, Nov 2008
fig 1: ciclo de vida da informação

No domínio militar essa adaptação foi conceptualizada essencialmente através de duas formas: pela equiparação da informação a qualquer outro recurso tangível, e pela criação de doutrina (Guerra da Informação), estabelecendo o seu modo de emprego de modo a se conseguir a desejada superioridade da informação. Este artigo não está focado no valor operacional da informação, mas sim nos processos internos das organizações e na forma de gerir a informação. Considerando as diferentes fases do ciclo de vida da informação (aquisição, exploração, disseminação e arquivamento) pode-se considerar que, enquanto a guerra da informação tem o focus na aquisição e exploração, a Gestão da Informação (GesInfo) foca-se ao nível da disseminação e arquivamento. Mais propriamente, o objecto deste artigo reporta-se ao manuseamento da



informação em Sistemas de Processamento Automático de Dados (ADP Systems). Portanto a "guerra" aqui consiste, por exemplo, na que frequentemente travamos para encontrar um ficheiro importante no computador que teima em não aparecer, ou quando queremos assegurar que numa organização a informação é devidamente partilhada e acessível em tempo oportuno a quem dela necessita.

> ***Segundo a NATO (A/C)322-D(2007), Gestão da Informação é a disciplina que dirige e suporta o manuseamento da informação durante o seu ciclo de vida, assegurando que esta se torna na informação certa, no formato adequado, de qualidade adequada e no timing certo, de forma a satisfazer as necessidades de uma organização.[1]***

1 Definição ligeiramente alterada pela Finabel, pelo acrescento do requisito "Timing adequado"

A análise dos princípios orientadores para a gestão da informação, é por si esclarecedora quanto à multiplicidade dos factores que concorrem para uma eficaz Gestão da Informação. Esses princípios[2] são:

- **A informação é um recurso corporativo**; a informação pertence à organização como um todo e não a um indivíduo ou seção em particular. Para a sua produção foram consumidos recursos da organização, pelo que deve ser gerida como qualquer outro recurso tangível.

- **A informação deve ser standardizada**; a standardização reduz o tempo de processamento e facilita a troca de informação entre utilizadores e sistemas.

- **A informação deve ser etiquetada**; A inclusão de de uma etiqueta contendo informação sobre os próprios dados (metadata) facilita a distribuição, o armazenamento e a recuperação da informação. Informação não etiquetada é informação perdida.

- **A informação deve ser criada uma vez**, mas utilizada muitas vezes; a reutilização da informação é por si só um elemento economizador de recursos, ao evitar os custos de a recrear novamente.

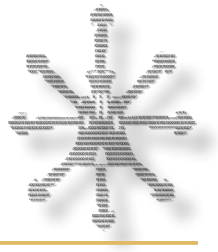
- **A informação deve ser disponibilizada no formato adequado**; a distribuição da informação num formato que permita a sua utilização imediata constitui um factor economizador do recurso "tempo".

- **A informação deve ser o mais difundida possivel**; dentro da organização deve estar acessível a qualquer entidade que dela necessite.

- **A informação tem um proprietário**; a posse da informação determina a responsabilidade pela produção e actualização da informação, mas não determina a difusão aos utilizadores, que terá por base o princípio da necessidade de aceder ou de conhecer.

- **A Gestão da Informação é uma responsabildade colectiva**; todas as entidades de uma organização tem

2 Princípios definidos pela Finabel, estudo R24R – Gestão da Informação Operacional, Nov 2008



responsabilidades na Gestão da Informação. A política de Gestão da Informação deve ser veiculada pela cadeia de comando.

- A informação deve ser segura; a segurança da informação compreende todas as componentes que potenciam a sua utilização eficaz. Estas incluem o princípio da autenticação, não repudiação, disponilbilidade, confidencialidade, integridade e proteção fisica.

- O processo de arquivamento deve facilitar a pesquisa.

- A informação deve cumprir com os requisitos legais.

- Os objectivos para a informação são determinados pelas necessidades operacionais.

Estes constituem os princípios gerais e universais para a gestão da informação, que de certa forma modelam as soluções que as organizações possam encontrar para assegurar uma Gestão da Informação eficaz. Alguns destes princípios enquadram-se no âmbito da responsabilidade individual de qualquer elemento da organização, outros têm um caracter mais geral e reportam à organização como um todo.

GESTÃO DA INFORMAÇÃO NUM QUARTEL GENERAL OPERACIONAL

Num Quartel General (QG) operacional o ambiente para a gestão da informação é relativamente estável e bem definido. Os principais atores estão associados às diferentes áreas funcionais, a hierarquia é conhecida, e as prioridades para a informação foram devidamente estabelecidas aquando do planeamento operacional, através da identificação dos elementos de informação essencial, crítica e prioritária para suporte à tomada de decisão pelo comandante.
O estabelecimento da organização para a gestão da informação é essencial. No topo da hierarquia está naturalmente o comandante, responsável pela definição da política de GesInfo; na base estão os utilizadores, ou mais propriamente os originadores ou destinatários da informação e, centralmente a esta estrutura, existe uma entidade responsável pela implementação da política de GesInfo estabelecida pelo comandante, a designada Célula de Gestão da Informação (IMC). Esta supervisa o cumprimento das normas estabelecidas, centraliza o manuseamento da informação e assume a gestão do sistema.

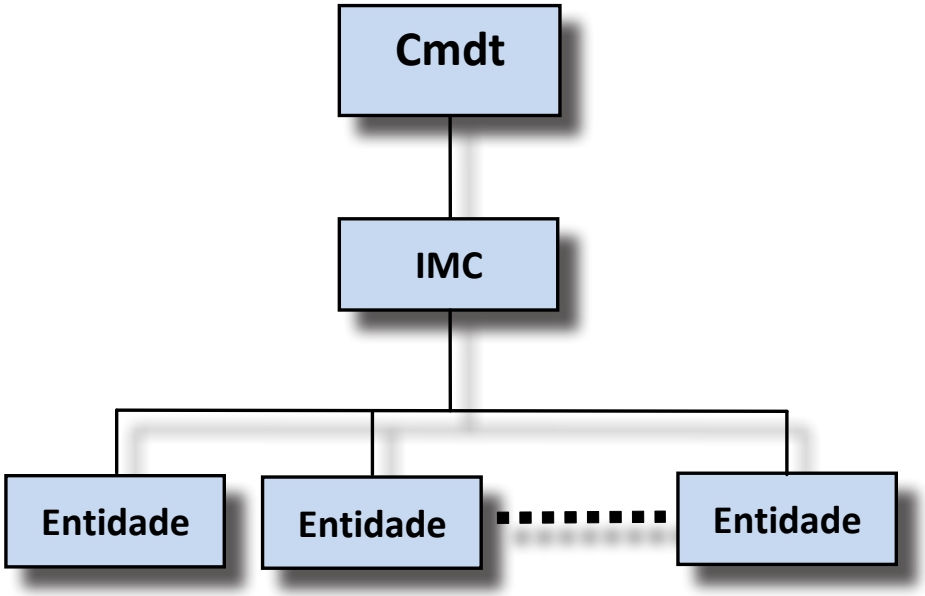


Fig 2: Organização para a Gestão da Informação

A MATRIZ DE REFERÊNCIA PARA A PARTILHA DA INFORMAÇÃO

Outgoing					EUROFOR FHQ																				Subordinate Units												
					COMMAND							OPS							SPT					Approval														
"O" Originator "D"Drafter "S" Sender "A" Action "I" Information "R" Registering "D" Daily "AN" As Necessary	SECURITY CLASS	PERIODICITY	OHQ	Area	LEGAD	PAO	JMA	XO	COS	FCdr	IMC	DCOS Ops	CJ2	CJ3	Futur OPS	CJOC	CJ5	CJ9	DCOS Spt	CJ1	CJ4	CJ6	CJ8	FCdr	DCOS OPS	DCOS SUPP	ACC	MCC	HQSU	INF BN	CAV SQN	FA Btr	Eng Coy	ROLE 2	ADA Plt	Hel Detach	TACP	NBC Plt	NSE
FRAGO	R	AN	I	CJ3	I	I		I	O	I	R/S	O	I	I	I	I	I	I	O	I	I	I	I	X			A/I	A/I	A/I	A/I	A/I	A/I	A/I	A/I	A/I	A/I	A/I	A/I	
EVENTREP	R	AN	A	CJ3		I			I	I	R	I	I	I	I	O/S		I	I	I	I	I	I		X		I	I	I	I	I	I	I	I	I	I	I	
INTSUM	C	D	A	CJ2	I	I	I	I	I	I	R	I	O/S	I	I	I	I	I	I	I	I	I		X			I	I	I	I	I	I	I				I	
INTREQ	C	AN	A	CJ2							R		O/S	I		I									X													
LOGASSESSREP	R	D	A	CJ4					I	I	R			I		I			I		O/S					X			I	I	I	I	I					I

Fig 3: Extrato da matriz para a partilha da informação
Fonte: EUROFOR, SOP " Information Management ", Jan 2011

Num QG o elemento central para a gestão da informação é a matriz com as necessidades de informação a partilhar (IER - Information Exchanging Requirements), na qual se identificam todos os documentos a partilhar, as entidades que os originam e os respectivos destinatários, as entidades que os aprovam e a periodicidade com que são elaborados. O sucesso para uma gestão eficaz da Informação passa pelo rigor na definição desta matriz, uma vez que esta constitui o guia orientador para o trabalho de todas as entidades envolvidas. Na prática existem duas matrizes, uma para os documentos que dão entrada e outra para os documentos que saem do QG.

O FLUXO DA INFORMAÇÃO

Tendo como referência a European Rapid Operational Force (EUROFOR), apresenta-se na figura 4. O fluxo da informação seguido no processo de certificação do QG do Battle Group disponibilizado para a EU durante o 2° semestre de 2011.
Os aspectos mais relevantes desta organização são os seguintes:

- todas as entidades envolvidas estão referenciadas (externas e internas à organização);

- cada área funcional tem um responsável pela GesInfo nessa área;

- controlo centralizado de toda a informação partilhada.

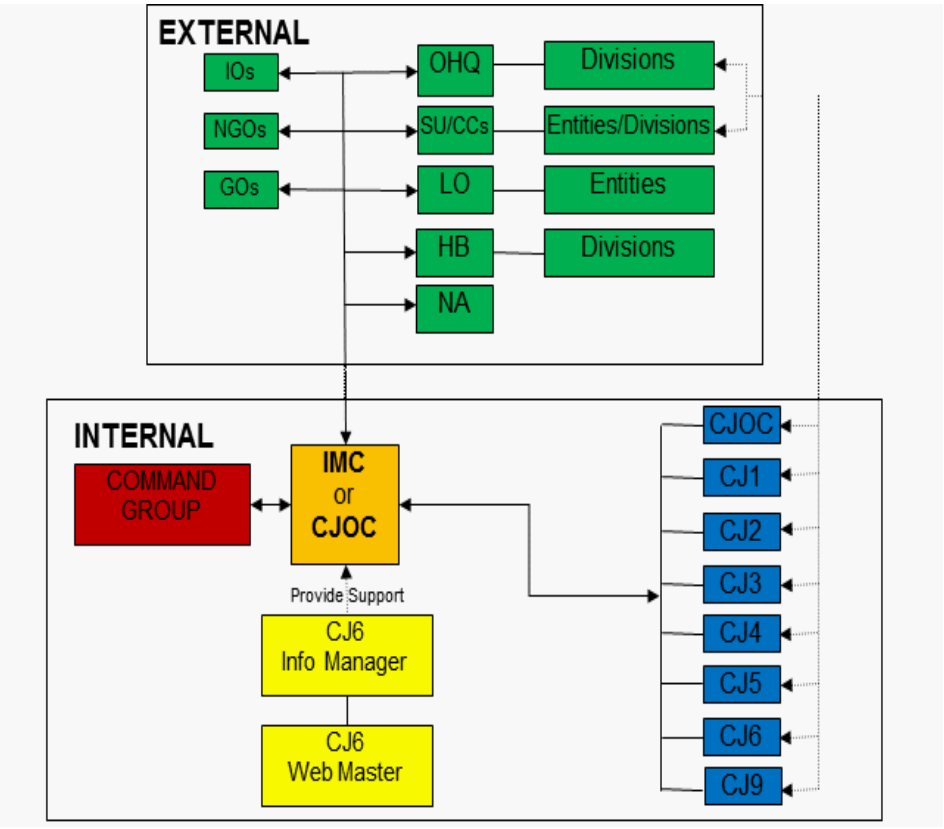


Fig 4: fluxo da informação num QG operacional
Fonte: EUROFOR , SOP " Information Management ", Jan 2011

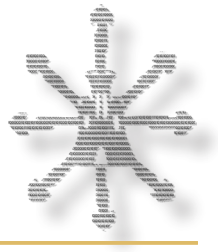
A CÉLULA DE GESTÃO DA INFORMAÇÃO

O ponto forte desta organização é o facto de se ajustar à natureza hierarquizada da organização militar. A existência de um ponto centralizador de toda a informação partilhada, quer interna quer externamente, permite facultar ao comandante o ponto de situação relativo a qualquer assunto, assim como implementar procedimentos de gestão da informação que permitam que se atinja o objectivo primeiro da GesInfo que é o de garantir que a informação chega aos destinatários no timing adequado e no formato apropriado para dela se poder fazer uso imediato.



fig 5: conceito para a Gestão da Informação
Fonte: EUROFOR, exercício BORA 11, fotos cedidas pelo PAO

O aparente ponto fraco consiste no estrangulamento potencial originado pela centralização num único ponto de toda a informação partilhada. Numa organização complexa, onde o ritmo de informação poderá ser frenético e a capacidade de resposta imediata constitui um imperativo, facilmente se imagina o estrangula-



mento previsível originado na IMC. Algumas condições concorrem para que tal não aconteça. Em primeiro lugar, não existe um ponto único, mas sim dois pontos. Um para a informação de rotina, que é de facto a IMC, que processa os relatórios que não são activadores de qualquer ação imediata, tais como relatórios de pessoal, logísticos etc. Outro para a informação relativa às Operações em curso, que é o Combined Joint Operations Center (CJOC). Para além disso, a IMC para alguns tipos de relatórios a expedir, funciona apenas como depositária, sendo estes enviados directamente pela respectiva área funcional. Enquadra-se neste último caso o acionamento de evacuações sanitárias originadas na Célula de Coordenação para a Evacuação de Pacientes (PECC).

Para além da organização do fluxo da informação, o trabalho na IMC terá que estar automatizado, através de um software específico que facilita os procedimentos de registo e envio dos documentos através do correio electrónico - Outlook. Na prática, esse software consiste numa digitalização da matriz IER, do qual se faz uma descrição funcional sumária no artigo seguinte: “Gestão da Informação – uma solução de software”

Bibliografia:

- Finabel, estudo R24R – Gestão da Informação Operacional, Nov 2008

- NATO, documento AC/322-D(2007)

- EUROFOR, Information Management SOP, Jan 2011

Gestão da Informação - Uma Solução de Software

A utilização do correio electrónico (Outlook) como meio universal de comunicação tornou-se uma prática em todas as organizações. Num Quartel General (QG) operacional de uma força projectável, por exemplo, onde normalmente se instala uma rede segura para a missão, o outlook assume mesmo o papel de principal meio para a comunicação, quer esta seja formal ou informal. Para além disso, toda a informação está na rede e é nesta que se centraliza toda a actividade, pelo que o sucesso da organização passa muito pela eficiente exploração das sua potencialidades. A gestão da Informação assume um papel de relevo nesse processo, pela otimização de tarefas e processos que são tranversais a toda a organização.

Na Europen Rapid and Operational Force, (EUROFOR) foi desenvolvido um software que implementa as boas práticas para a gestão da informação, satisfaz as necessidades de um QG operacional, ao mesmo tempo que facilita o trabalho do utilizador de sistemas computorizados. Desse software, apresentam-se neste artigo as características gerais, omitindo os detalhes técnicos e de gestão, focando-se apenas a sua componente funcional. Esta solução revelou excelentes resultados no exercício BORA 2011, que culminou o aprontamento e a certificação da EUROFOR como Force Headquarters (F)HQ para o battle group da União Europeia (ERF EUBG 2011-2). Foi igualmente utilizada durante o exercício Dragão-Padrela-Orion 2011, realizado também no âmbito da preparação do Batalhão Português integrante do ERF EUBG 2011-2.

REQUISITOS FUNCIONAIS

A caracterização geral deste sistema pode-se efectuar pela análise dos seus requisitos funcionais, os quais se podem agregar nas seguintes áreas:

- Centralização da informação: toda a informação relevante para uma organização, quer se trate de informação trocada com entidades externas, ou se reporte a coordenações internas, aparece disponível num único local.

- Utilização distribuída e gestão centralizada: funcionamento numa Rede de Area Local (LAN) por qualquer utilizador da rede e gestão centralizada do ambiente para a informação.

- Flexível e adaptável a qualquer organização: a natureza e tipo dados a gerir é irrelevante, uma vez que a standardização reporta-se apenas ao nome dos ficheiros e não ao seu conteúdo. Compete ao gestor a parametrização do sistema de forma a satisfazer as necessidades da organização.

- Informação standard: o nome dos ficheiros segue uma norma que obriga à inclusão de informação sobre o conteúdo dos ficheiros tais como a data, o originador, a natureza dos dados que contém, etc.

- User friendly: a aplicação tem por objectivo constituir um facilitador do manuseamento de documentos digitalizados, integrando funcionalidades de aplicações do Microsof Office e do sistema operativo Windows.

O NOME STANDARD PARA OS FICHEIROS

A standardização do nome dos ficheiros determina a arquitectura base de todo o sistema. Este está concebido de forma a forçar que todos os ficheiros sejam guardados no arquivo digital segundo determinadas regras gerais. Essas regras também estabelecem o formato do nome dos ficheiros e qual a informação relativamente aos dados que o ficheiro contém (metadata), deve constar no nome. Adicionalmente, automatiza as tarefas inerentes ao arquivamento dos documentos digitalizados. Numa analogia com o sistema de catalogação de uma biblioteca, este sistema proporciona uma funcionalidade similar, mas aplicável à informação armazenada num sistema computorizado.
Tomando como exemplo o seguinte nome de ficheiro, vejamos a quantidade de informação que esse nome proporciona:

120224-G3-99-FRAGO_5-ORION-U

Adicionalmente, o nome também indica que este documento está arquivado no arquivo geral digitalizado da organização. Existe uma cópia na pasta dedicada ao originador "G3", outra cópia na pasta dedicada a todas as ordens parcelares, outra cópia dedicada aos documentos relativos ao "Processo ORION" e, eventualmente, numa outra pasta (sub processo), caso este tenha sido atribuído aquando do registo do documento.

Data de criação: **24 Fevereiro 2012**

Originador: **G3**

Nº Registo: **99**

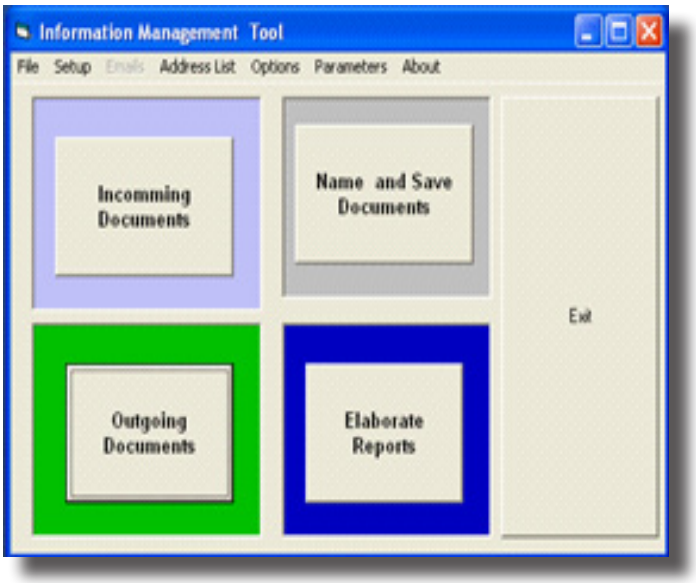
Typo de Documento: **FRAGO**

Nº sequencial para o tipo: **5**

Assunto: **ORION**

Classificação de segurança: **NAOCLAS (U)**

VISÃO FUNCIONAL DO SOFTWARE



O utilizador poderá efectuar qualquer uma das seguintes tarefas principais:

- Registar um documento que deu entrada na organização;

- Registar um documento que foi emitido pela organização;

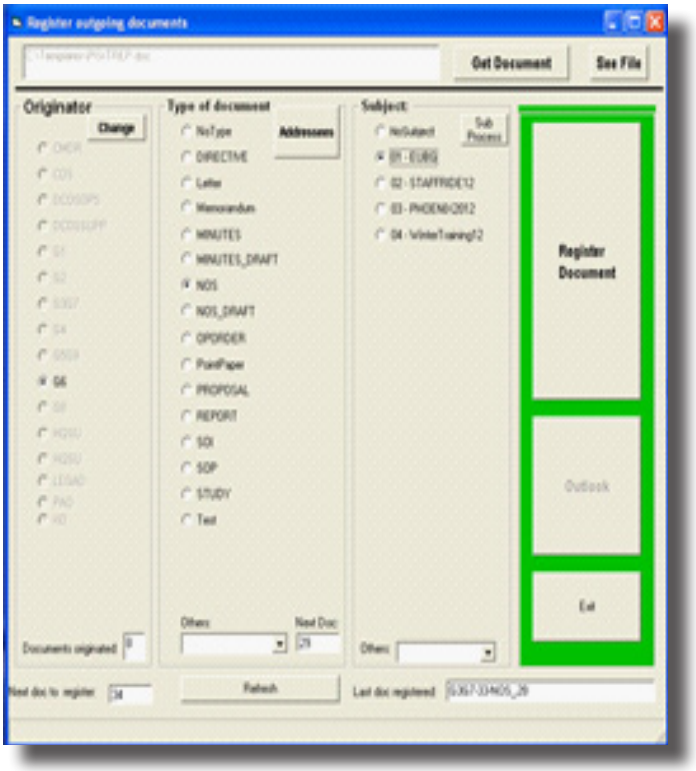
- Atribuir um nome a determinado documento seguindo as regras pré-definidas, e arquivá-lo em pastas pré-definidas;

- Aceder aos templates standard dos documentos a elaborar (personalizáveis para cada utilizador).

Estas funcionalidades são personalizáveis de acordo com as necessidades do utilizador, ou seja, cada utilizador só terá acesso às funcionalidades atribuídas ao ser perfil.

Registo de um documento

O utilizador procede ao registo do documento, sendo este arquivado nas respectivas pastas. Após o registo poderá enviá-lo através do Outlook, podendo os destinatários estar previamente definidos.



1. Selecciona o documento a registar;

2. Selecciona o originador do documento;

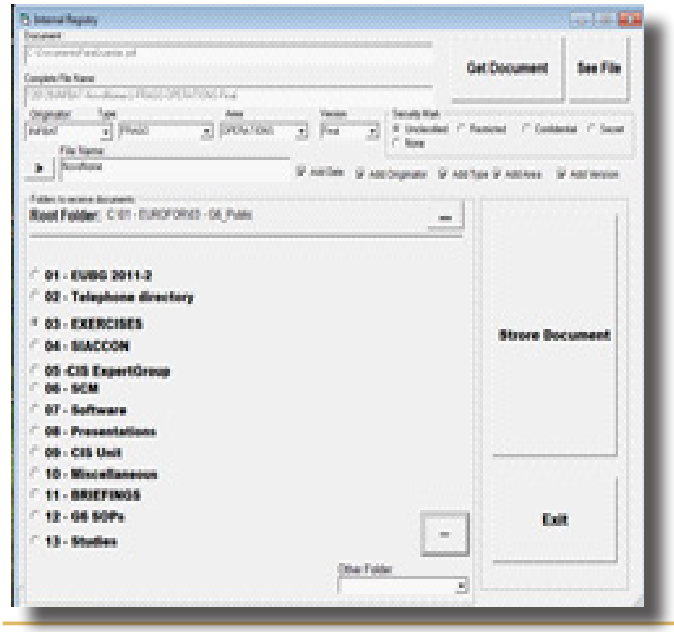
3. Selecciona o tipo de documento;

4. Atribui o processo e o subprocesso;

5. Procede ao registo;

6. Acede ao Outlook, tirando proveito da parametrização do sistema, nomeadamente pelo prenchimento automático dos destinatários, pré-definidos para o tipo de documento seleccionado ou para listas gerais de destinatários.

Atribuir nome formatado a um documento



Permite a renomeação automática de um ficheiro de acordo com a norma semelhante à utilizada para documentos registados.

1. Seleccionar o documento;

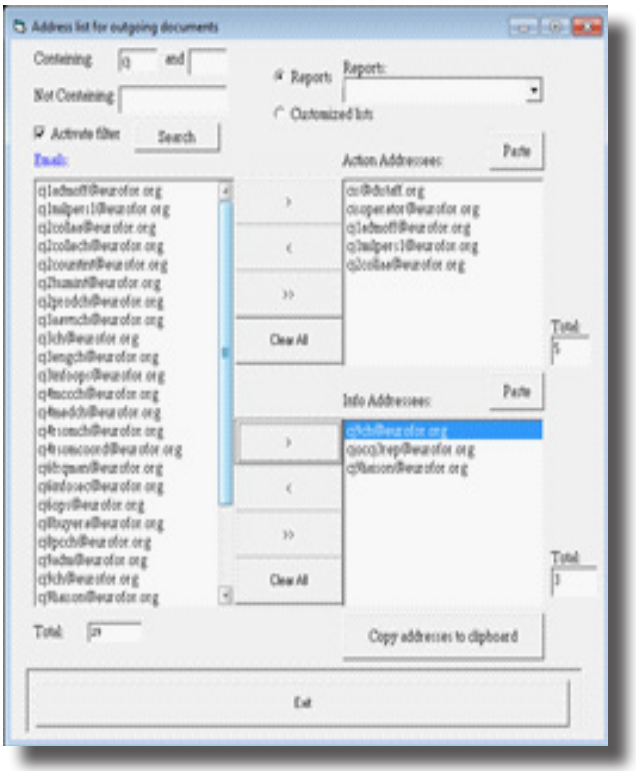
2. Atribuir-lhe um assunto;

3. Parametrizar os campos que devem constar no nome;

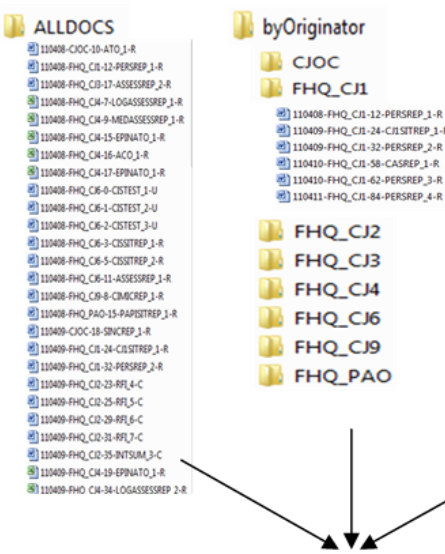
4. Gravar na pasta desejada.

Gestão de endereços do Outlook

O acesso a endereços do Outlook torna-se tarefa árdua quando, em presença de um grande número de endereços, é necessário seleccionar entidades pertencentes a um grupo específico, como por exemplo: todos os elementos da mesma área funcional.
O utilizador pode utilizar filtros para seleccionar os endereços pretendidos, criando a sua própria lista e exportá-la para o Outlook (através do clipboard do Windows).
Esta funcionalidade é particularmente útil em exercícios, dado que os endereços são criados com base na afinidade de funções.



O arquivo digital



Arquivo geral relativo aos documentos expedidos, organizado por origem e por tipo de documento



Arquivo organizado por assunto

À esquerda: arquivo geral digital relativo aos documentos expedidos, originado pelo software de GesInfo durante o exercício BORA 2011.

À direita: arquivo digital originado pelo software de GesInfo, organizado por assunto. Neste caso reporta-se ao QG da EUROFOR no início de 2012.

Novo conceito de Centro de Comunicações



TCor Tm (Eng.) João Garcia

1. Introdução

As alterações profundas de operar e proceder à interligação dos meios de Comunicações e Sistemas de Informação (CSI) proporcionam formas diferenciadas da transmissão da informação entre as forças, quer elas integrem o Sistema de Forças Nacional (SFN), quer em missões internacionais como Forças Nacionais Destacadas (FND) em operações humanitárias e de apoio à paz.

A infraestrutura CSI que apoia a preparação e sustentação da componente operacional do SFN permite que os utilizadores interajam, utilizando de uma forma transparente todos os meios de comunicações, reduzindo ao mínimo a noção de operador de transmissões e de dependência de um centro de comunicações.

Os meios CSI, utilizados numa vertente de operações de campanha, estão a aproximar-se à integração total dos serviços, permitindo fornecer a todos os utilizadores os diferentes serviços de voz, mensagens, dados e imagem, proporcionando vantagens técnicas que se convertam num fator complementar da força no campo de batalha.

A organização de um Centro de Comunicações (CCom) exige uma estreita coordenação com os comandantes e seu Estado-Maior (EM), com órgãos de unidades de transmissões do escalão superior, subordinadas e ainda com unidades adjacentes tanto em tempo de paz como numa situação tática, onde os serviços a instalar no CCom dependem da missão da unidade a apoiar, do pessoal e dos recursos a serem afetos ou autorizados.

A definição de um Centro de Comunicações, utilizada nos manuais escolares, como sendo um "conjunto de meios de transmissões de natureza diferente (pessoal e material), instalados, operados e mantidos por pessoal da arma de Transmissões", obriga a que os CCom devam ser reorganizados pela imposição das dificuldades da gestão de recursos humanos e de materiais.

A própria definição de CCom, encontrada no manual da exploração de transmissões, definida como o "conjunto de meios de comunicações de natureza diferente e de meios de coordenação e apoio, guarnecidos, instalados na proximidade uns dos outros, encarregado e responsável por aceitar, preparar para transmissão, receber e entregar mensagens", apresenta uma falha conceptual e necessita uma transformação profunda de conceitos adaptados à área CSI.

Neste sentido, vamos estudar os possíveis CCom que podem ser organizados no Exército e preparar a definição geral de CCom, centrando a atenção principalmente em três tipos possíveis de centros, a saber:

- Os CCom do SIC-Op;

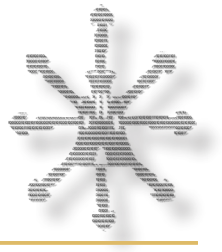
- Os CCom do SIC-T;

- Os CCom de apoio às operações das Brigadas.

2. Os Sistemas de Informação e Comunicações

Os Sistemas de Informação e Comunicações (SIC) do Exército Português devem possuir a capacidade de se adaptarem rapidamente a ambientes dinâmicos, proporcionando aos comandantes a informação essencial onde esta é fundamental e quando é necessária. Essa informação deve ser protegida da intercessão e utilização indevida por forças oponentes e ser apresentada ao utilizador num formato percetível e relevante.

Os SIC permitem à força aproveitar oportunidades e ir de encontro aos objetivos da missão. Os modernos SIC, como o Sistema de Informação e Comunicações Operacional (SIC-Op) e Sistema de Informação e Comunicações Táticos (SIC-T), abrangem um alargado leque de funções relacionadas com o tratamento da informação.



Estas funções, face às novas formas de requalificação no atual ambiente operacional em rede, podem ser sintetizadas nas seguintes classificações: a aquisição (elementos essências da informação são introduzidos no SIC), o processamento (sequência de operações efetuada sobre uma informação com o objetivo de produzir um resultado final específico), a armazenagem (consiste na retenção, organização e disposição de dados), o transporte (capacidade dos SIC para suportar a troca e disseminação da informação), o controlo (com a função de dirigir, monitorizar e regular as outras funções do SIC), a salvaguarda de Informação [1] (confiança que se obtém pela aplicação de um conjunto das medidas destinadas a proteger as comunicações, a informação e outros sistemas eletrónicos e não eletrónicos, e ainda a informação que é armazenada, processada ou transmitida nestes sistemas, garantido a confidencialidade, integridade, disponibilidade, não-repúdio e autenticação) e a apresentação (imposição final onde os sistemas interagem com os utilizadores).

Como todas as áreas do conhecimento, os modernos sistemas de informação e meios de comunicação devem ser regidos por princípios como a interoperabilidade, a "commonality" (visa que os equipamentos e sistemas possam ser operados e mantidos por pessoal com formação em qualquer um dos sistemas, e quando os seus sobresselentes e consumíveis podem ser trocados entre si), a compatibilidade, a normalização, a ligação, a agilidade e a confiança.

A importância do conteúdo da informação é primordial para a organização, o que faz com que a grande preocupação deva ser a forma como pode ser rapidamente integrada na instituição Exército e no seu modelo organizacional.

Não é o propósito deste artigo debruçar-se sobre os conceitos do tema "gestão de mensagens", apenas apontar uma seta num hipotético paralelismo da já sobejamente conhecida "gestão documental", da mesma forma que a informação que percorre os circuitos dos SIC tem necessariamente de ter um sentido de utilidade, ser precisa e eficaz, o que só acontecerá se estiver ordenada, classificada e arquivada devidamente.

3. O Sistema de Informação e Comunicações Operacional

O SIC-Op do Exército Português tem uma estrutura organizada e delineada para apoiar a preparação e sustentação das forças da componente operacional do sistema de forças e para o cumprimento das missões particulares aprovadas, de missões reguladas por legislação própria e de outras missões de natureza operacional.

A evolução das tecnologias de informação e de comunicações, que se tem vindo a verificar, proporciona às comunicações o desempenho de um papel de relevo no seio dos Exércitos. O sucesso das operações, agora "centradas em rede", torna-se cada vez mais dependente de informações precisas, oportunas, completas e fiáveis, só possível com um SIC sólido, eficaz e seguro, o que leva a que este tipo de sistemas assuma uma maior importância na tomada de decisão.

1 Information Assurance



a. Conceito da Infraestrutura CSI

A infraestrutura do SIC-Op tem como base uma rede malhada assente em nós de comunicações interligados por um sistema de transmissão apoiado em links de feixes hertzianos digitais ou em fibra ótica. A ligação desses nós às UEO é feita através de links de feixes hertzianos digitais ou fibra ótica, seguindo uma estrutura em estrela.
O SIC-Op fomenta o conceito de "Operações Centradas em Rede"[1] , de forma a dotar todo o Exército Português com uma capacidade de Comando e Controlo (C2), moderna, permanente, adaptada e adaptável.

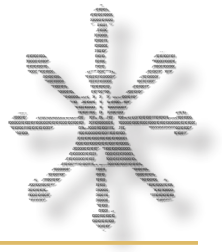
O SIC-Op integra um conjunto de infraestruturas espalhadas pelo Território Nacional, Ilhas e FND que incluem um conjunto diversificado de torres e antenas, um extenso parque de centrais de telecomunicações, servidores de comunicações, routers, switches, gateways, multiplexers e equipamentos de cifra, para além de um complexo parque de computadores.

b. Organização CSI para apoio do Exército

O Exército na sua estrutura organizacional tem uma Direção de Comunicações e Sistemas de Informação (DCSI) incluída na dependência do Comando das Forças Terrestres (CFT), que no âmbito da área CSI, é responsável por estudar, planear, dirigir e executar as atividades nas áreas das comunicações, sistemas e tecnologias de informação e da segurança.
A atividade que é exercida no seu âmbito é essencialmente a de contribuir para a capacidade de Comando, Controlo e Comunicações (C3) da componente terrestre, assegurar a instalação, configuração, operação e sustentação das infraestruturas de comunicações e dos sistemas de informação, em apoio da componente fixa, e definir os requisitos técnicos e de sistema que garantam a compatibilidade e a interoperabilidade conjunta e combinada dos diferentes sistemas.
O Regimento de Transmissões[2] (RTm), na dependência hierárquica da DCSI, tem a missão de instalar emanter o Sistema de Comunicações, de Informação e de Segurança da Informação do Exército, em articulação com o Centro de Dados de Defesa e a DCSI. Tem na sua estrutura orgânica o Batalhão de Comunicações e Sistemas de Informação e o Centro de Segurança da Informação.

1 Network Centric Warfare

2 In QO de pessoal da UEO



Através do Batalhão de Comunicações e Sistemas de Informação, assegura a manutenção das infraestruturas físicas de sistemas de informação e tecnologias de informação e comunicação das UEO e opera os si mas de gestão de comunicações e de informação.
O Centro de Segurança da Informação contribui para as Operações de Informação/Guerra de C2, nas suas vertentes de Segurança da Informação e Computer Network Operations.

c. O Centro de Comunicações de apoio a uma UEO

1 - Um novo conceito de centro

As definições apresentadas de um Centro de Comunicações como sendo um conjunto de meios de transmissões instalados, operados e mantidos por pessoal da arma de Transmissões necessitam ser reformuladas, no sentido de reorganizar os CCom prevendo as dificuldades na gestão de pessoal e dos recursos de material, acrescido das especificidades das novas tecnologias de informação que permitem uma maior capacidade de gestão e de interação dos meios de comunicações e sistemas de informação.

O Centro tem como legado a instalação, operação e o manuseamento das mensagens, local onde se processa a gestão e controlo de todo o tráfego escrito, se verifica o tráfego recebido e se reencaminha ou entrega aos destinatários, e ainda onde são operados e geridos os meios utilizados na transmissão e receção da informação.

A composição tipificada para um CCom, com a integração do conceito de centro de telecomunicações, é essencialmente a de se constituir como um órgão organizado em centro de mensagens, central telegráfica, central telefónica, central rádio e centro cripto. No entanto, a integração das funções da central telegráfica e do centro cripto, ocorrida desde o ano 2000, deu origem a um novo órgão que obteve a designação de Centro de Processamento de Mensagens (CPM).
O conceito do CCom, organizado em vários centros, operados de forma diferenciada e exigindo formação específica na operação dos meios, tem de ser abandonado, de forma a permitir que um CCom que apoia uma UEO funcione com um número reduzido de operadores com capacidades diversificadas, permitindo o seu aproveitamento num maior universo de atividades.

As conceções mais modernas de CSI são assentes em plataformas que executam a transmissão da informação através da comutação em rede e em equipamentos e tecnologias que garantem a total interoperabilidade e integração nos SIC; a descentralização de meios e o aumento de capacidades está estreitamente ligada às crescentes necessidades de troca de informação e na disponibilização dos serviços de voz, dados e vídeo a todos os utilizadores que operam em rede.
A segurança é uma vertente fundamental da salvaguarda dos recursos e das pessoas, assim como de toda a estrutura organizacional do Exército. A definição de políticas de segurança e a introdução de protocolos e serviços de segurança em redes, acrescida dos sistemas de criptografia, permitem efetuar uma gestão de segurança da informação que vai evitar a modificação não-autorizada de dados ou informações, armazenados, em processamento ou em trânsito.

Assim, podemos partir para um novo conceito de Centro de Comunicações abrangente e sofisticado, em que as tecnologias de informação tenham o seu impacto nos meios a serem utilizados e os recursos, por sua vez, serem geridos com eficiência e eficácia, potenciando as competências e a operacionalização. Desta forma, podemos apresentar a seguinte definição generalista de CCom:
Órgão responsável pela organização e operação dos meios associados aos sistemas de informação e comunicações, com vista a disponibilizar todos os serviços de voz, dados e vídeo que garantam a transmissão da informação cumprindo os requisitos de segurança.

2- Organização do CCom

Os CCom devem ser organizados reforçando as características e as funcionalidades que estão na competência, atribuições e missão da arma de transmissões, por conseguinte, os meios possíveis de disponibilizar ao C2 de uma UEO podem ser reorganizados num compromisso entre os QO de pessoal e a estrutura funcional existentes nas UEO.

Como temos conhecimento, desde o ano 2000, que dois dos órgãos dos CCom, o centro cripto e a central telegráfica, coexistem na mesma sala com os requisitos de segurança militar definidos no SEGMIL-1, tendo sido designada essa estrutura como CPM e, conjuntamente com o centro de mensagens, a central telefónica e a central rádio constituíam o CCom. Com a nova definição de CCom e o conceito de CSI no transporte da informação, os órgãos de um centro podem ser redefinidos, potencializando os recursos humanos e materiais e os espaços disponibilizados para a gestão dos meios CSI das UEO.

Desta forma, com o novo conceito de CCom podemos efetivar uma reorganização do centro em dois órgãos:

– O Centro de Processamento de Mensagens (CPM), que concentra as funções da Central Telegráfica (CTeleg), do Centro de Mensagens (CMens) e do Centro Cripto (CCp);

– O Centro RádioTelefónico (CRT), que reúne as funcionalidades da Central Rádio (CRádio) e da Central Telefónica (CTelef).

Na figura 1 é representado um modelo de disposição dos dois órgãos, o CPM e o CRT, numa perspetiva de concentração dos meios em salas com condições, em termos de área e de segurança, adequadas aos meios a serem instalados e ao seu modo de funcionamento.

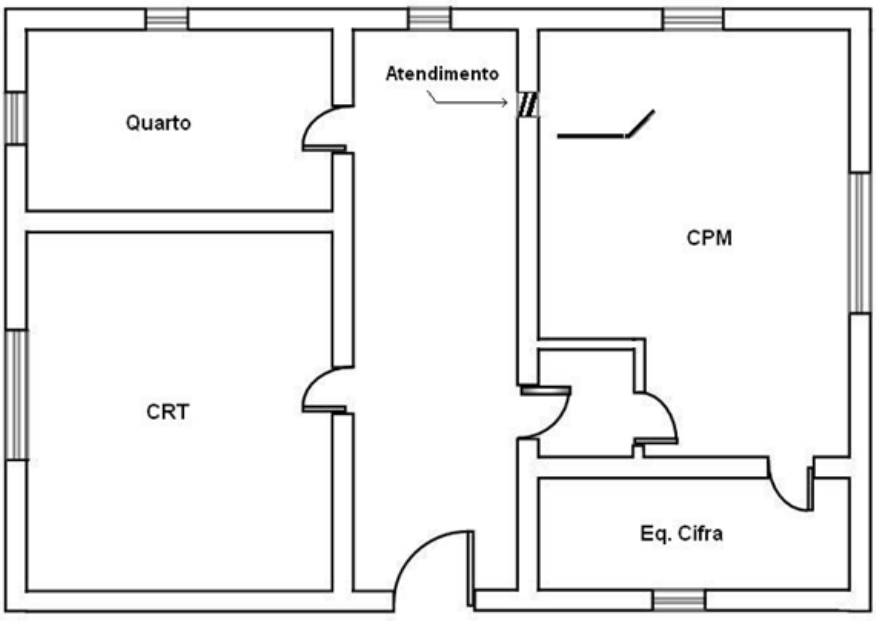
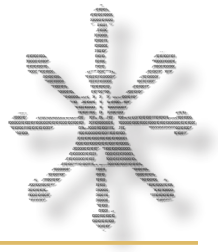


Figura 1 - Planta base de um CCom



a - O Centro de Processamento de Mensagens

Este Centro tem como missão específica a gestão das mensagens manuseadas e processadas no CCom, tendo as seguintes funções principais:

– Gerir e controlar todos os documentos escritos que passam pelo CCom;

– Conferir o tráfego recebido, procedendo ao seu reencaminhamento ou entregá-lo aos destinatários;

– Processar o tráfego a expedir, distribuindo-o pelos meios a serem utilizados na sua transmissão;

– Manusear os documentos em suporte digital ou em pa pel, cumprindo os requisitos de segurança;

– Arquivar os documentos em suporte digital ou em papel em locais próprios.

b - O Centro Rádiotelefónico

O CRT opera os meios de comunicações, explorando as redes rádio e a rede telefónica da UEO, este centro pode coexistir na mesma sala que o CPM, na sua impossibilidade, quando o serviço o exigir, o atendimento geral da UEO pode ser reencaminhado para uma extensão da sala do CPM.

As tarefas que um CCom tem de efetuar nomeadamente a de receber, carimbar, protocolar, distribuir, registar, classificar e arquivar as mensagens, não podem continuar a ter tamanha complexidade, exige uma mudança e um controlo dos fluxos baseados em plataformas exigentes de novas tecnologias de informação. Só assim, é possível partir-se para soluções com automatismos de transmissão, de arquivo e organização de mensagens e processos em formato eletrónico, bem como o controlo do seu estado e/ou localização em qualquer instante.

Realçar a importância dos arquivos no Exército passa, necessariamente pela sua definição, que engloba todo o conjunto de documentos, independentemente da sua natureza ou suporte, arrecadados ao longo dos tempos, e da reflexão e compreensão do seu significado. Quantos de nós não estivemos na situação infrutuosa de dizer “nunca ouvi falar” desse assunto, este percalço deixa de ter significado quando a resposta for “vai pesquisar no arquivo”.

4. O Sistema de Informação e Comunicações Táticos

O SIC-T é um sistema de comunicações planeado e organizado para apoio de uma unidade em campanha, garantindo a ligação entre o comandante e os vários comandos subordinados.
Este sistema proporciona aos elementos da componente operacional, comunicações e sistemas de informação, tendo em vista uma total adaptação e integração no conceito de "Operações Centradas em Rede", o que permite aos diferentes escalões obter uma apresentação comum da situação operacional permanentemente atualizada, como base essencial para a avaliação das operações e do C2 da situação operacional.
Organizado com uma estrutura modular, flexível, segura e preparada para proporcionar ao comando, às informações, à logística e às unidades de combate uma excelente mobilidade e a adaptabilidade necessária às novas exigências do campo de batalha, apresenta como primordial proficiência o domínio da interoperabilidade em operações conjuntas e combinadas, bem como com os sistemas de comunicações fixos, e complementarmente com a capacidade de transportar a informação em ambientes seguros.
Permite satisfazer os requisitos de economia, de projeção da força e de rentabilização de meios e recursos, dando resposta a uma maior possibilidade **de missões, com um número reduzido de meios humanos e materiais.**

a. Arquitetura do SIC-T

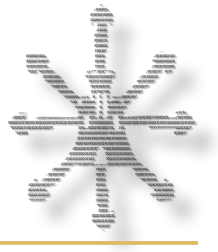
Este sistema está orientado para os serviços que se pretendem ter disponibilizados em cada um dos escalões de forças. Cada nível operacional é apoiado por um ou mais módulos CSI, com as potencialidades que garantem um conjunto de capacidades, que se traduzem na disponibilidade dos serviços aos elementos localizados num Posto de Comando (PC), mas também na garantia dos links de comunicações entre os diferentes



níveis operacionais, ou pela constituição de uma estrutura de rede malhada baseada no conceito de apoio de comunicações de área para utilização em operações convencionais.
O SIC-T[1] enquadra-se nos objetivos da transformação da NATO ao nível da Information Superiority e do Network-Enabled Capabilities. Desenhado em torno da tecnologia IP[2] , a arquitetura do sistema permite a implementação de uma disposição modular ajustável e flexível, nomeadamente na capacidade de operar num alargado espectro de operações e tipologia de conflitos, na capacidade de trabalhar em ambiente de rede, no garante da fácil integração das forças de combate, de apoio de combate e logísticas, no permitir o dimensionamento da força em conformidade com a missão e em assegurar a inter-

1 In relatório final do projeto inicial de implementação do SIC-T, CFT/DCSI, Nov06

2 Internet protocol



operabilidade em cenários conjuntos e combinados. A arquitetura do SIC-T[4], na sua componente de comunicações táticas foi desenhada para ser expandida pela área de operações interligando todas as componentes das forças de uma brigada, e inclui os seguintes Sub-sistemas:

- SAE - Sub-sistema de Área Estendida[1] que representa a ligação central (backbone) da rede, composta por um conjunto de nós de comutação, interligados basicamente por links rádio multicanal, que assegura o acesso às redes do SIC-OP, SICOM[2] e às redes civis e NATO;

- SAL – Sub-sistema de Área Local[3] proporciona, a um determinado grupo de utilizadores, os diversos serviços de voz, dados e vídeo;

- SUM - Sub-sistema de Utilizadores Móveis[4] destina-se a apoiar os utilizadores dispersados pela área de operações;

- SSR – Subsistema de Segurança de Rede implementa diferentes níveis de segurança nas diferentes áreas de rede do SIC-T (RED e BLACK);

- SGR – Sub-sistema de Gestão de Rede[5] responsável pela gestão, administração e monitorização da rede.

O SIC-T altera o panorama do apoio de CSI às operações táticas, garantindo que a tecnologia permita a integração dos sistemas, de uma forma modular, sistémica e dinâmica de acordo com as necessidades de cada operação e em qualquer momento, permitindo a redução de meios, a integração de novas tecnologias, a interoperabilidade, em operações conjuntas e combinadas, a inserção de Centros de Comunicações de Batalhão (CCB), e o despontar do Centro de Comunicações de Companhia (CCC) como uma estrutura ligeira, adaptada à mobilidade natural deste escalão.

b. O Conceito de CCom do SIC-T

O SIC-T apresenta uma capacidade real de integração operacional, para um melhor e mais eficaz desempenho nas operações militares terrestres, explorando as novas tecnologias associadas às comunicações, aos computadores, sensores e sistemas de armas.
A descentralização de meios e o aumento de capacidades desconcentradas está estreitamente ligada às crescentes necessidades de troca de informação e rapidez com que é executada. Isto vai exigir mais responsabilidade e consequentemente mais formação dos utilizadores, já que estes meios estão disponíveis na orgânica dos Batalhões e Companhias, e deverão fornecer aos utilizadores os diferentes serviços de voz, dados e vídeo, totalmente integrados.
O desaparecimento dos centros de comunicações organizados da forma tradicional, anunciam o fim de uma filosofia de apoio. Todo o fluxo de informação de um SIC moderno é veiculado pelos servidores e bases de dados disponíveis no sistema, permitindo uma economia de meios humanos e materiais expressiva.

1 WAS - Wide Area Subsystem

2 istema Integrado de Comunicações Militares

3 LAS- Local Area Subsystem

4 MS - Mobile Subsystem

5 SMCS - System Management and Control SubSystem

O SIC-T vai proporcionar aos Comandantes e ao EM das unidades operacionais vários serviços, dos quais se destacam o correio eletrónico, o SICCE (Sistema de Informação para o C2 do Exército), o AFADTS (Advanced Field Artillery Tactical Data System), o MMHS (Military Message Handling System), a Intranet, a telefonia, o vídeo, o File Server LAN e WAN, os Antivírus/Atualizações de Software e o Sistema Tracking.
O apoio de CSI através deste sistema foi desenhado para distinguir dois CCom distintos nas suas capacidades, mas semelhantes nas suas possibilidades de apoio CSI a uma força:

- O Centro de Comunicações de Batalhão (CCB) que serve o PC do batalhão, é constituído basicamente por duas cabines, uma de transmissão e outra para o C2 e Gestão (C2 & G), que são organizadas de forma a proporcionar o acesso ao sistema, inserindo-se nos nós e nas redes, facilitando a integração de todos os utilizadores e estabelecer as ligações com as unidades adjacentes.
- O Centro de Comunicações de Companhia (CCC) com uma estrutura bastante mais ligeira que a do CCB, serve o PC da Companhia, sendo compatível com a mobilidade característica desta subunidade. É constituído apenas por uma única cabine que, para além de permitir a instalação dos equipamentos de comunicações, tem ainda integrada uma componente de energia e mastros, tornando-o muito móvel.

Neste novo esquema, figura 2, o BTm e a CTm são responsáveis pela instalação, exploração e manutenção de todos os sistemas de comutação/roteamento e transporte de sinal. Os utilizadores são quem instalam, exploram e mantêm os próprios equipamentos.

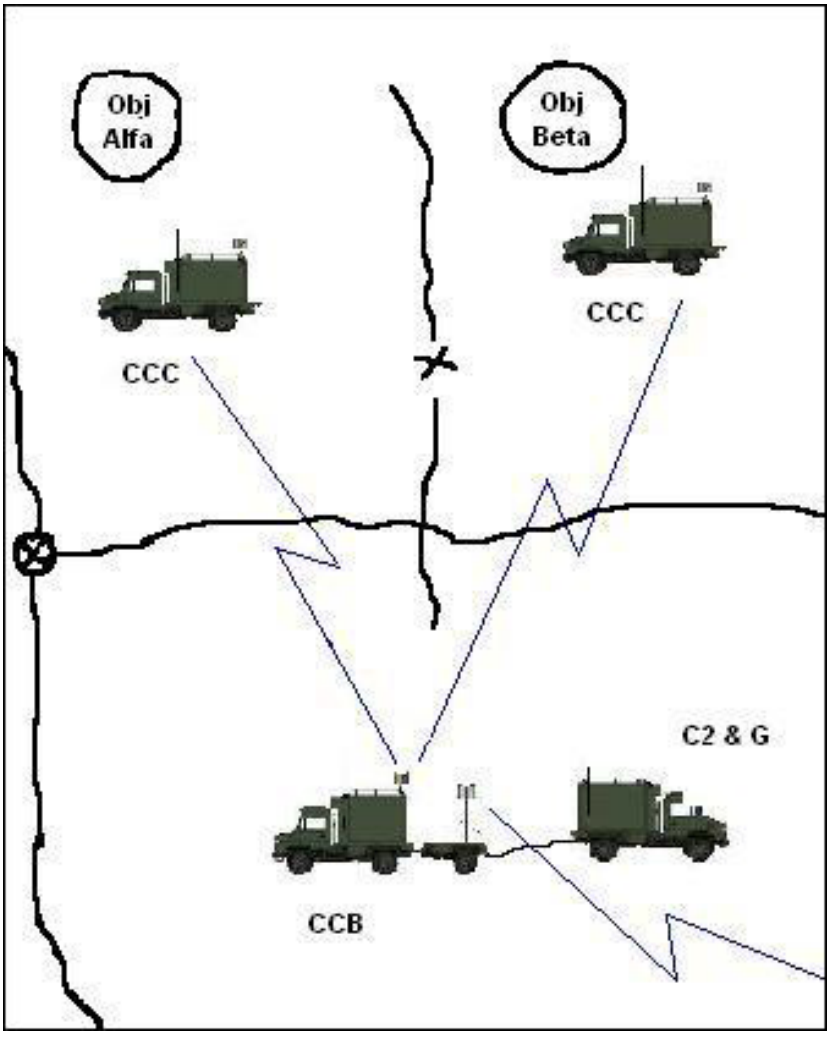


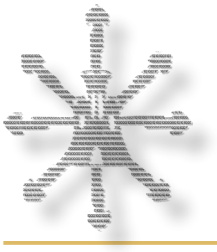
Figura 2 - Organização do SIC_T

Novo conceito de Centro de Comunicações

Os utilizadores serão todos os militares a quem seja atribuído um terminal de uma qualquer aplicação. A responsabilidade de operação dos terminais de utilizador fica a cargo dos militares a quem estes forem distribuídos, como exemplo pode referir-se o SICCE, que não será operado por operadores formados especificamente para esse fim, mas sim pelo militar cuja função implique a atribuição de um terminal desta aplicação.

O novo conceito de CCom apresentado anteriormente não é alterado face às diferenças substanciais referidas para o apoio CSI de uma UEO ou de uma força apoiada por um sistema orientado e alicerçado na disponibilização de serviços.





5. Organização CSI de apoio às Brigadas

A estrutura CSI de apoio a uma Brigada é desenhada para estabelecer essencialmente o funcionamento em rede dos Batalhões Operacionais, das Companhias Operacionais, dos PC de Brigada, dos módulos para projeção de FND e das Companhias de Transmissões. A unidade escalão tipo para apoio de uma Brigada em operações num teatro, em treino operacional e em exercícios é o Batalhão, no entanto, a Brigada tem organicamente uma Companhia de Transmissões para apoio na área CSI.

a. As unidades de apoio em comunicações

O Exército tem, como um dos pilares indispensável ao C2, as unidades de transmissões, que estão organizadas para apoiar o treino e o emprego das forças e estão preparadas com as condições necessárias para que cumpram as missões que lhe estão atribuídas e lhe permitam conduzir e participar nas várias operações. A unidade que tem como missão principal instalar e manter o SIC-T, necessário ao exercício do C2 de uma Brigada, e prestar apoio em caso de empenhamento num Teatro de Operações (TO), é o Comando do Batalhão de Transmissões[1] (BTm) que está vocacionada para empregar e garantir o apoio CSI a uma Brigada e integra o sistema de comando que compreende três níveis; as Comunicações que visam o transporte da informação, a Informação necessária para a tomada da decisão e o C2 que apoia o Comandante na tomada da decisão e no controlo das operações. A Companhia de Transmissões de Apoio[1] (CTmAp) integra o sistema de C2, caracterizado pela integração e direção de todos os outros sistemas, é uma unidade das Forças de Apoio Geral vocacionada para garantir apoio adicional em comunicações. Está preparada para garantir o apoio em comunicações a todas as forças do SFN que não disponham de Unidade de apoio CSI e assegurar o apoio adicional em comunicações a uma Brigada quando a área de operações assim o exigir.

As Companhias de Transmissões orgânicas de uma Brigada têm como missão a de instalar e manter o SIC-T, necessário ao exercício do C2, assegurar o seu funcionamento e apoiar em comunicações os PC de Brigada.

Esta assegura o funcionamento do SIC-T, necessário ao exercício do C2 da Brigada, se as necessidades operacionais não exigirem o emprego de um Batalhão de Transmissões e estabelece ligação entre o Comando e as subunidades da Brigada.

b. Os CCom de Apoio de uma Brigada

De acordo com os documentos de referência, podemos encontrar os conceitos de apoio baseados na instalação de dois tipos de CCom para apoio de uma brigada, o CCom de Comando e o de Área.

O CCom de Comando destina-se a apoiar um PC específico, sendo solidário com os seus deslocamentos. Apoia também, na medida do possível, determinadas unidades localizadas nas suas imediações.

O CCom de Área apoia uma determinada área, servindo todas as unidades que nela se encontrem ou que por lá transitem e que necessitem de apoio.

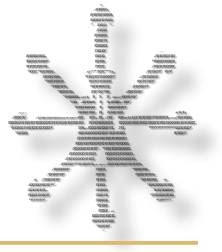
O deslocamento desses centros faz-se de acordo com alterações significativas do dispositivo tático adotado para uma determinada situação.

A organização de qualquer um dos CCom definidos para apoiar uma Brigada tem sempre em conta todos os princípios enunciados anteriormente, bem como as características da evolução tecnológica que permitem a flexibilização, a automatização e a interoperabilidade dos meios e dos recursos existentes e os coloca permanentemente disponíveis.

Um CCom instala, mantém e opera fundamentalmente a infraestrutura de comunicações que integra todos os meios disponíveis, colocando à disposição de todos os utilizadores das redes a instalar, os serviços de voz, de dados, os meios rádio, os feixes hertzianos (FHz) e os equipamentos de segurança necessários para o transporte da informação.

O CCom permite que os utilizadores tenham acesso aos meios de comunicações fundamentais para o C2 das operações, tais como a rede telefónica, o correio eletrónico, o serviço de mensagens, os rádios, a

1 In QO de pessoal da UEO



cifra, a vídeoconferência e o SICCE, e assim proporcionar a interligação entre os CCom e entre todos os utilizadores das unidades da Brigada.

Nas responsabilidades da instalação dos meios da área CSI, dentro do quadro das operações em rede, deve ser considerada a seguinte sequência de procedimentos; a implementação, a configuração e controlo e reconfiguração da rede, e finalmente assegurar os requisitos de segurança.
Um CCom de apoio às operações de uma Brigada deve ser preparado para instalar os meios e equipamentos de forma a apoiar o funcionamento das seguintes redes e sistemas:

(1) Sistemas de Informação de Comando e Controlo

- (a) Sistema de Informação para o Comando e Controlo do Exército (SICCE).
- (b) Web Information Services Environment (WISE).
- (c) Correio Eletrónico.
- (d) Vídeo-Conferência (VTC).

(2) Comunicações de Voz

- (a) Rede Rádio VHF/FM
- (b) Rede Telefónica de Campanha

(3) Comunicações Seguras

(4) Sistemas de Comunicações

- (a) Rede Telefónica de Campanha.
- (b) Redes Rádio VHF/FM.
- (c) Rede Rádio HF de Comando.

O CCom de apoio de uma brigada, apesar das redes a serem instaladas e dos conceitos encontrados nos manuais escolares, não alteram o propósito de renovar o conceito de CCom, pois as companhias das brigadas ainda a operar os equipamentos de décadas, estão a conseguir organizar o apoio CSI de acordo com o conceito de disponibilização de serviços de voz, dados e vídeo, numa tentativa de aproximar o conceito de apoio com as características e possibilidades das novas tecnologias de informação e aos sistemas de informação e comunicações (SIC-Op e SIC-T) apresentados anteriormente.

6. Conclusões

Com vista a contribuir para o conceito de CCom e sua organização, foi estudada e esquematizada toda a envolvente relativa às noções de apoio da área CSI e das estruturas organizacionais CSI do Exército. A arquitetura, a organização e a articulação entre os SIC do Exército permitem definir e reduzir os recursos que estão envolvidos na prestação do apoio, e assim, contribuir para a simplificação da missão da Arma de Transmissões.
Subsiste uma certa dificuldade em prever o impacto das novas tecnologias de informação, embora se possam antever alguns contornos de excelência, como a maior facilidade e rapidez de acesso à informação, a coordenação eficaz de utilizadores, que se encontram dispersos geograficamente, o C2 das operações e a participação nas atividades de gestão dos recursos.
As novas tecnologias favorecem a tendência para que as forças não detenham fronteiras demarcadas em relação ao campo de batalha e permitam operar os meios cada vez mais “em rede”, interligando-se com outras forças e, dentro delas, com os seus utilizadores, operando cada vez mais ligados em tempo real. Este facto impõe uma grande mudança de comportamentos e de atitudes por parte dos utilizadores e decisores do sistema.
Os recursos humanos constituem um recurso estratégico, em virtude da elevada criatividade que possuem e do potencial que representam, por isso, devido ao seu valor e grande escassez, é necessário



que sejam considerados como um investimento, devendo apostar-se na formação e no treino.

O apoio de comunicações tem atualmente um significado diferente do utilizado num conceito de utilização dos meios e de concentração de centros específicos na sua operacionalização, em que determinadas tarefas são executadas por elementos da arma de transmissões.

O apoio em comunicações e sistemas de informação deverá ser prestado através da implementação em rede, assente em equipamentos e tecnologias que garantam a total interoperabilidade e integração nos SIC e a continuidade de uma gestão integrada de forma a disponibilizar os serviços de voz, dados e vídeo a todos os utilizadores que operam na rede.

A produção e aperfeiçoamento dos sistemas de arquivos e de recuperação de dados, gestão de correio e telecomunicações, produção e manutenção de aplicações de documentos essenciais é um caminho a percorrer no sentido de tornar úteis as funções que exercemos e acautelar eventuais negligências da conservação em memória (arquivamento).

O sentimento de segurança contribui para dar credibilidade às capacidades e potencialidades dos sistemas. Mais do que um simples produto ou tecnologia, que se pode adquirir, aplicar e esquecer, a segurança deverá ser encarada de forma integrada com as necessidades imperativas do Exército, vistas como um processo em permanente evolução que requer uma enorme capacidade para provocar e gerir mudanças, tanto nas rotinas e comportamentos, como nas infraestruturas tecnológicas e organizativas.

Com o novo conceito de Centro de Comunicações definido de uma forma genérica, pretende-se abraçar uma nova fase das transmissões, apresentando a nova ideia de apoio CSI e ainda a introdução de um novo “modus operandi”, baseado na disponibilização dos serviços de voz, dados e vídeo através dos meios de transmissão operados pelas unidades de transmissões, tornando-se, por conseguinte, importante e urgente a inserção nos manuais escolares deste novo conceito.

"Desconflituar" – A Estrutura ISTAR e a Guerra Eletrónica

"O que habilita o Sábio soberano ….. a conseguir as coisas fora do alcance do homem comum é o conhecimento prévio"
Sun Tzu



TCor Tm (Eng.) Marques da Silva

INTRODUÇÃO

A Guerra Eletrónica (GE) e a estrutura de Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR), tal como a maioria dos sistemas militares e civis, sofreram o impacto da evolução tecnológica, situação que exponenciou o acesso aos meios de comunicações e torna estas atividades cada vez mais dependentes das Tecnologias de Informação (TI). Os computadores, as comunicações e a informação, formam a componente base da maioria dos sistemas militares, em especial das Informações, Vigilância, Reconhecimento (ISR)[1] e da Guerra Electrónica. Esta crescente dependência das TI introduz, novas oportunidades que podem ser exploradas e novas vulnerabilidades que devem ser acauteladas.

Este novo ambiente exige o estabelecimento de princípios e de uma estreita coordenação entre a GE e a estrutura ISTAR (E-ISTAR), no âmbito do planeamento e da condução das atividades militares, de forma que as mesmas possam integrar e contribuir para moldar o processo de targeting (aquisição de objetivos) e direcionar a forma como as informações podem apoiar as diferentes operações militares.

As atividades da GE e ISTAR, conjugadas com o uso das TI, contribuem para melhorar a compreensão da situação operacional, desempenhando ambas uma função integradora das operações de informação, relevante para a eficácia do cumprimento da missão.

A INFORMAÇÃO E AS INFORMAÇÕES

Julgamos oportuno começar por clarificar o âmbito dos conceitos de informação e informações. A **informação** consiste num único elemento de dados ou numa série ou grupo de dados que são captados por um sensor e posteriormente recolhidos por outro tipo de meio.

A informação é a declaração do estado das coisas existentes, ou que existiram algures no espaço e no tempo. Tem natureza inequívoca e pode relacionar eventos do passado ou do presente, assumindo carácter histórico ou actual. É definida como "dados não processados de cada evento, que podem ser utilizados na produção de informações[2]" O comandante, durante a preparação do processo de decisão, deve ser capaz de identificar qual o tipo e a relevância da informação que tem ou pretende vir a ter disponível, de forma a construir o seu plano. As perguntas às quais necessita de dar resposta constituem-se como Requisitos Críticos de Informação do Comandante (CCIR- Commander's Critical Information Requirements), a partir dos quais a componente de informações desenvolve os Requisitos de Informações Prioritários (PIR - Priority Intelligence Requirements). Estes constituem-se nas questões chave (de informações) para as quais o comandante deve ter respostas, de forma a auxiliar o processo de decisão e a elaboração do plano operacional. Informação isolada é um facto ou uma série de factos, mas quando aquela informação é relacionada com outra informação e considerada à luz da experiência do passado, dará origem a um novo conjunto de factos com a designação de **informações**.

1 ISR - Intelligence, Surveillance and Reconnaissance.

2 Definição adaptada do AAP-6 - NATO Glossary of Terms and Definitions.

As informações diferem da informação porque, sendo o resultado de um processo de apreciação subjectiva, não é inequívoca e está aberta à contestação. O relacionamento de conjuntos de informação, ou a avaliação comparativa da informação com base em dados de conhecimento já erigidos, e a elaboração das respectivas conclusões por um analista constitui o "processo" de análise, que é a raiz da produção de informações a partir da informação. As Informações são assim "o produto resultante do processamento e análise da informação sobre nações estrangeiras, "forças" hostis ou potencialmente hostis, elementos e áreas de operações atuais ou potenciais[1]" . A simplicidade da relação entre dados, informação e informações é mostrada em forma de diagrama na figura 1.

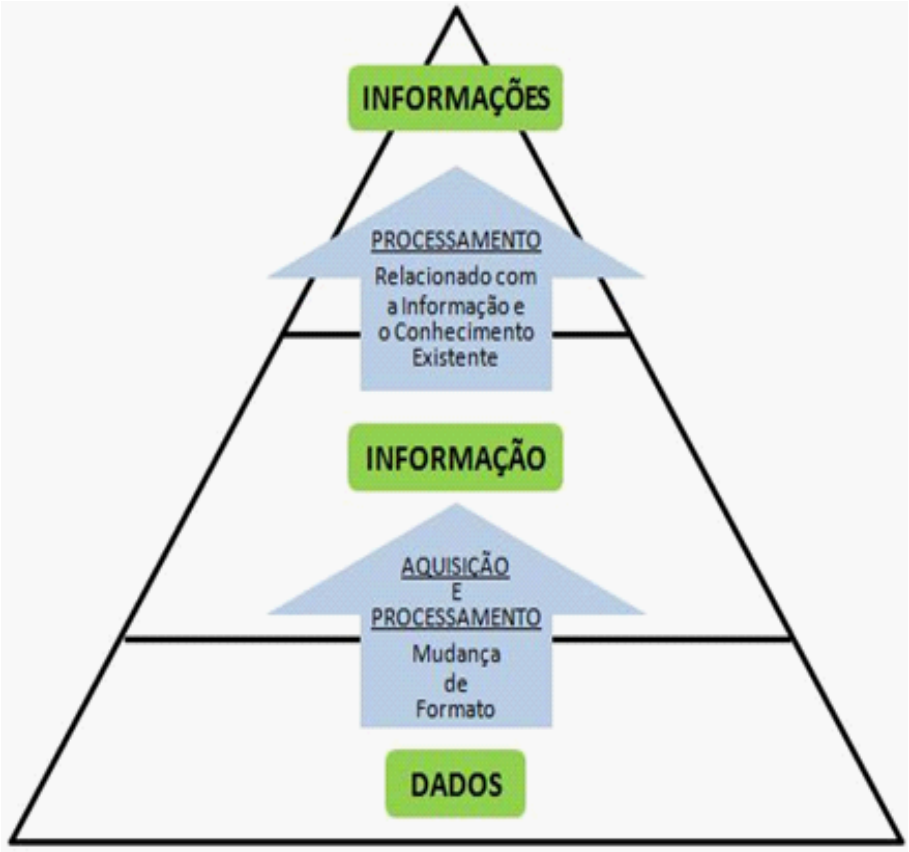


Figura 1 – Relação entre Informação e Informações
(Adapatado: AJP 2.0 - Intelligence, Counter Intelligence and Security)

1 Definição adaptada do AAP-6.

AS ACTIVIDADES DE INFORMAÇÕES, VIGILÂNCIA E RECONHECIMENTO (ISR)

As Informações fornecem ao comandante uma previsão das actividades do adversário, das suas táticas prováveis, ou uma avaliação das suas capacidades. A posse de informações proporciona-lhe uma vantagem nítida sobre o adversário, habilita-o a "entrar" na mente do seu oponente e a formar uma visão das ações ou reações que o seu adversário provavelmente terá. O comandante pode planear as suas ações com base neste conhecimento, diminuindo os riscos inerentes ao combate e consequentemente aumentar as suas probabilidades de sucesso.

O Ciclo das Informações - Para lidar com toda a informação disponível é necessário conduzir uma série de operações, sistematicamente estruturadas, de forma a identificar qual a relevante, procurar a que não está presente e processar a adequada, tornando a informação em Informações, antes de a distribuir. O ciclo das Informações é o enquadramento para a realização de quatro operações que culminam na distribuição do produto acabado das Informações. A sequência daquelas operações tem uma natureza cíclica, uma vez que as Informações requerem a reavaliação e atualização constante, para se manterem atuais e relevantes face às necessidades do comandante. Quando a informação começa a ser processada e disseminada como Informações, aquelas operações irão sobrepor-se, sendo realizadas simultânea e continuamente em vez de forma sequencial. As operações são usualmente conduzidas em quatro fases (Orientação, Aquisição, Processamento e Disseminação) conforme é mostrado esquematicamente na figura 2. O Ciclo das Informações reflete assim o processo pelo qual a informação é coligida, convertida em Informações e tornada acessível aos utilizadores.



Figura 2 – Ciclo das Informações
(Adapatado: AJP 2.0 - Intelligence, Counter Intelligence and Security)



A Vigilância é a observação sistemática de áreas da superfície, do subsolo e aeroespaciais, mas também de lugares, pessoas ou coisas, por meios visuais, sonoros, eletrónicos, fotográficos, ou outros. A vigilância do campo de batalha é a observação sistemática da área de operações, com a finalidade de fornecer informação oportuna que possa ser transformada em Informações de combate.

O Reconhecimento é a missão realizada para obter, pela observação visual ou outros métodos de detecção, informação sobre as atividades e recursos de um adversário ou potencial adversário, ou para obter dados fiáveis relativos às características meteorológicas, hidrográficas, ou geográficas de uma área particular.

Os meios de reconhecimento e vigilância adquirem assim a informação que se transforma em Informações, quando processada, analisada, avaliada e interpretada. A aquisição de Informações é efectuada por um conjunto de diferentes disciplinas (fontes de Informações) que a seguir se descriminam:

- **Signal Intelligence** (SIGINT) – São Informações derivadas da interceção de comunicações (COMINT)[1] e outras emissões electrónicas (ELINT)[2] . As SIGINT são utilizadas para interceptar emissões electromagnéticas e para fornecer informação sobre as capacidades, intenções, organização e locais de "forças" adversárias.

- **Imagery Intelligence** (IMINT) - São Informações derivadas de imagens adquiridas a partir de sensores com base em plataformas terrestres, marítimas, aéreas ou espaciais.

- **Human Intelligence** (HUMINT) - São uma categoria de Informações recolhidas e fornecidas por fontes humanas.

- **Open Source Intelligence** (OSINT) - São Informações derivadas da informação pública disponível, ou outra informação não classificada que tenha distribuição ou acesso limitado.

- **Acoustic Intelligence** (ACOUSTINT) – São Informações derivadas da aquisição e processamento de fenómenos acústicos.

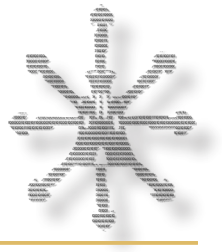
- **Measurement and Signature Intelligence** (MASINT) – São Informações científicas e técnicas, obtidas a partir da análise quantitativa e qualitativa dos dados derivados de instrumentos sensíveis, com a finalidade de identificar qualquer característica distintiva associada à fonte emissora ou ao remetente, para facilitar a sua identificação e/ou a sua medição posterior.

ACTIVIDADE DE GUERRA ELECTRÓNICA

A GE tem uma ampla aplicação nas operações militares. O efeito da actividade de GE pode ser temporário ou permanente e tem o potencial de minimizar o uso da força, evitando assim baixas e danos colaterais desnecessários. O **Ataque Eletrónico** permite neutralizar as funções de comando e/ou atacar as tecnologias de informação. Apoia ainda outras actividades de operações de informação, nomeadamente a decepção e as operações psicológicas, nomeadamente a radiodifusão para audiências alvo. As **Medidas de Proteção Eletrónica**, em conjunção com a gestão do espectro electromagnético, contribuem para combater a capacidade de um adversário transmitir informação hostil e proteger o uso do espectro electromagnético pelas nossas tropas. As Medidas de Apoio Eletrónico são parte integrante da aquisição de informação e disponibilizam ao comandante uma grande variedade de informação a partir da adopção de medidas e soluções eficazes para a aquisição de objectivos.

1 COMINT - consiste na informação resultante da interceptação, monitorização e localização dos sistemas de comunicações adversários.

2 ELINT - consiste na informação resultante da interceptação, monitorização e localização dos emissores de não-comunicações adversários.



A GE pode ainda apoiar as operações, através da destruição da informação crítica, na qual o adversário iria fundamentar a sua decisão, ou através da degradação do sistema de comunicações para transporte da referida informação, o que se tornará numa vantagem para as nossas "forças".
A GE constitui assim uma ação militar, que explora a energia electromagnética para proporcionar a compreensão da situação operacional e obter efeitos ofensivos e defensivos no âmbito da manobra. Para além do ataque eletrónico, já referido anteriormente, a GE compreende a defesa eletrónica e a vigilância eletrónica, através do recurso das medidas de protecção e de apoio eletrónico.
A **Vigilância Eletrónica** (VE) é a utilização de energia electromagnética para fornecer informações e apoiar na compreensão da situação operacional. Baseia-se nas medidas de apoio eletrónico e Signal Intelligence (SIGINT) como fontes essenciais. A combinação destas duas actividades aumenta o espectro de actuação e o resultado operacional final.

A NATO, em determinadas operações, constitui o Centro de Operações de GE e SIGINT (SEWOC - SIGINT and EW Operation Center) cuja missão é proporcionar sincronização, coordenação, aconselhamento e apoio às operações de GE e SIGINT no ambiente electromagnético, enquanto se constitui como centro de apoio, em tempo real, ao comandante da "força" no alerta de ameaças, na análise de informações, na informação sobre objectivos, nas tácticas e nas contra-medidas.
O SEWOC materializa e coordena, desta forma, a principal actividade da GE, podendo no entanto a GE, ser também utilizada como tarefa secundária, envolvendo meios com capacidade para contribuir para a vigilância eletrónica, nomeadamente ao nível de estruturas e meios ISTAR.

UMA ESTRUTURA ISTAR

Intelligence, Surveillance, Target Acquisition, and Reconnaissance (ISTAR), é um processo que articula vigilância, reconhecimento, sistemas de aquisição de objetivos e sensores, no desenho da manobra e dos meios ofensivos e ou defensivos Abrange a pesquisa (aquisição) e a gestão da informação e das Informações, de forma que estas possam contribuir para a compreensão da situação operacional, para a condução das operações (pelo comandante e estado-maior) e no apoio do processo de aquisição de objectivos[1].
Uma Estrutura ISTAR (E-ISTAR)[2] deve integrar as atividades de Informações com a Vigilância, a Aquisição de Objetivos, o Reconhecimento e outras fontes de informação, que habilitem melhorar o conhecimento do Comandante sobre a situação e acelerem o Operational Planning Process (OPP). A E-ISTAR pode fazer a "ponte" entre as Informações de nível estratégico, onde podemos encontrar sistemas militares ou civis, nacionais ou estrangeiros, e os meios ISTAR das componentes de uma força operacional que coordena e orienta o esforço de pesquisa numa determinada área.
No âmbito de uma força operacional, a E-ISTAR desenvolve e coordena as atividades de Informações tanto a nível de estado-maior como ao nível dos sensores[3]. Este arranjo fornece uma cobertura contínua da área de responsabilidade das Informações, o que permite responder rapidamente às necessidades de Informações dos comandantes das unidades apoiadas. A missão genérica de uma E-ISTAR é a de apoiar em Informações e "targeting" (aquisição de objetivos), todo o espectro de operações.

1 Definição adaptada do AJP 2.7 – Doctrine for Reconnaissance and Surveillance.

2 A E-ISTAR aqui apresentada, tem como referência estrutura Holandesa do Joint Intelligence Surveillance Target Acquisition and Reconnaissance Command.

3 Os sensores tecnológicos podem geralmente ser divididos nas categorias sensores com imagem e sem imagem. Ambas operam no espectro eletromagnético e acústico e cobrem frequências não perceptíveis pelo olho ou ouvido humano. Os Sensores tecnológicos não fazem apenas a aquisição, têm também capacidade para gravar, transmitir e realçar determinado tipos de dados.

Para responder a esta missão, apresenta uma orgânica com base nas seguintes componentes funcionais: Comando e Controlo (Intel Fusion Cell); Guerra Eletrónica; Reconhecimento; HUMINT; IMINT; OSINT e Mapas/GIS. A E-ISTAR de referência, não individualiza em componente funcional as disciplinas de ACOUSTINT e MASINT.
O estado-maior da E-ISTAR apresenta as seguintes áreas funcionais:

- Área de operações correntes - responsável por estabelecer a coordenação com os sensores das diferentes componentes no terreno, através da atribuição de tarefas de pesquisa e receção dos dados e informação proveniente daqueles sensores.

- Área de Análise (ASIC- All Source Intelligence Cell) – Garante a gestão das bases de dados e efetua o processamento, análise, avaliação e interpretação da informação recolhida pelos sensores transformando-a em Informações. Nesta área, com exceção dos militares responsáveis pela gestão das bases de dados, os analistas são militares altamente especializados, normalmente licenciados e especialistas nas áreas: política, militar, económica, social, cultural, infraestruturas e de informação.

- Área de Comando e Controlo – Garante o apoio à decisão do comandante e a integração das duas áreas anteriores. Dispõe de uma área onde é trabalhado o Sistema de Informação Geográfica (GIS) de apoio à célula de Intel Fusion, conforme esquema apresentado na figura 3.

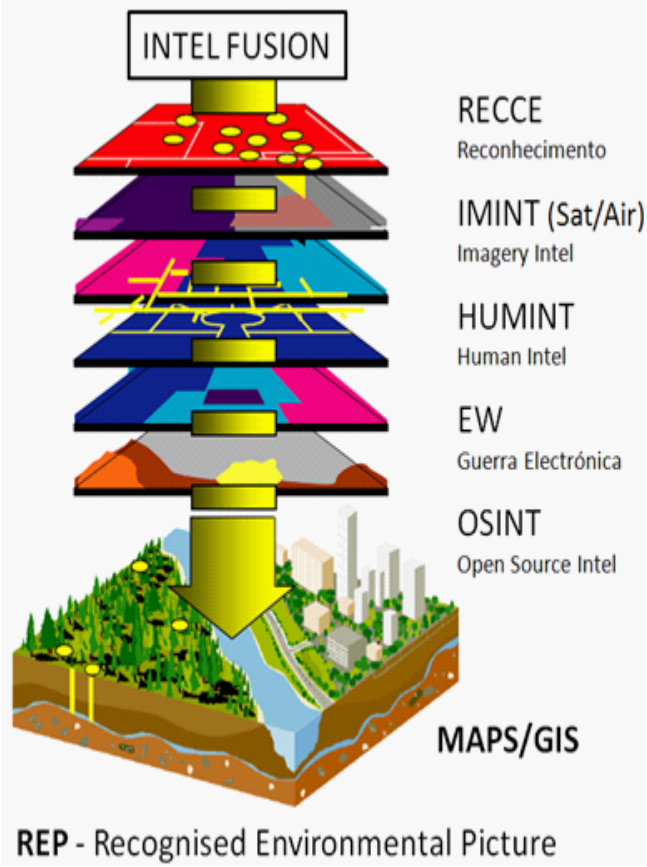


Figura 3 - Processo de Construção da Recognized Enviromental Picture
(Adaptado: Apresentação do JISTATC)

A atividade de comando e estado-maior da E-ISTAR é conduzida em consonância com os ciclos e processos de comando e controlo (OODA Loop - Observar, Orientar, Decidir e Agir) e das Informações (OAPD – Orientação, Aquisição, Processamento e Disseminação). O conceito implementado pela E-ISTAR tem como base a teorias de gestão de processos, e parte do pressuposto de que para cada atividade existe um processo primário e um processo de suporte que no caso da atividade ISTAR é desempenhado respetivamente pelas células ASIC e Ops. Desta forma no posto de comando da E-ISTAR os ciclos de Comando e Controlo (C2) e de Informações são integrados. O ciclo das Informações é sobreposto no ciclo de C2, formando dois triângulos sobrepostos, conforme mostra a figura 4, os quais servem de referência àquelas atividades e materializam dois canais complementares, o canal de comando e o canal técnico.

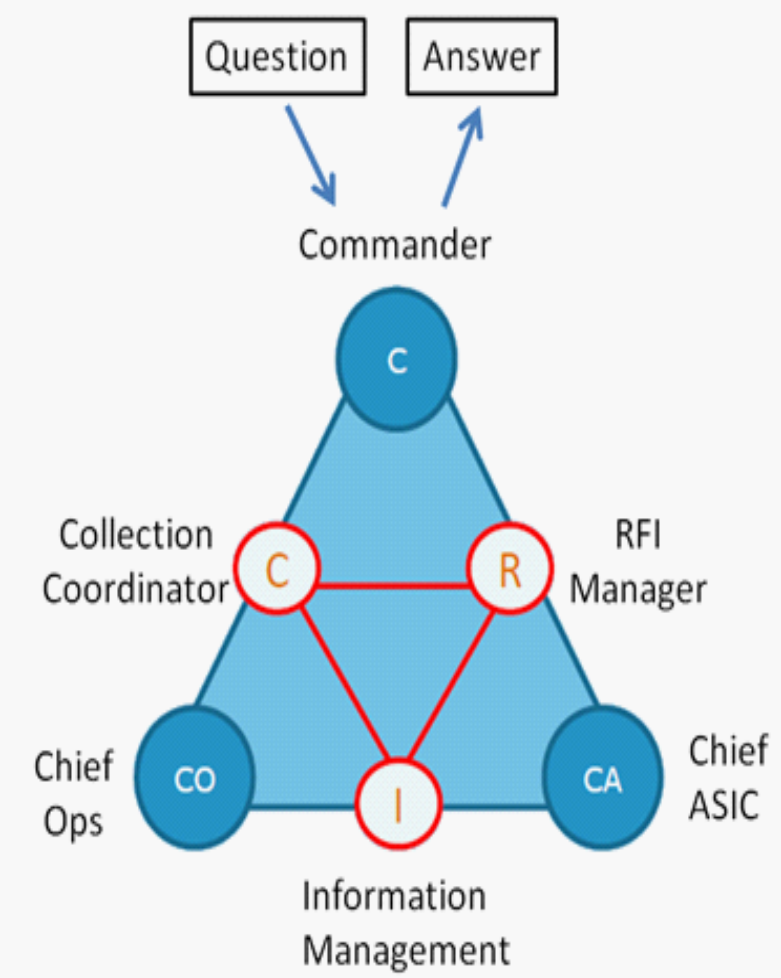


Figura 4 -Atividade de Comando e Controlo do Módulo ISTAR
(Adaptado: Apresentação do JISTATC)



- **No canal de Comando**: O comandante da "força" apoiada estabelece os seus Prioritary Information Requirements (PIR) sob a forma de perguntas que são transformados pelo Comandante da E-ISTAR (C) em Requests for Information (RFI), o Chief OPS (CO) canaliza a pesquisa para satisfazer o pedido, orientando os sensores adequados para obter a informação. Uma vez obtida esta informação, a mesma é disponibilizada ao Chief ASIC (CA) que analisa a informação recolhida, relaciona-a com a informação já existente e fornece respostas ao Comandante (C) para que este possa responder ao comandante da "força" apoiada.

- **No canal técnico**: os elementos envolvidos concentram em si competências de coordenação de sensores (C), acompanhamento do estado dos RFI (R) e de Gestão da Informação (I). O RFI Manager em coordenação com o chefe do ASIC (CA) e a célula de gestão da informação (I) verificam se têm capacidade de dar respostas imediatas aos PIR levantados pelo comandante da força apoiada. Caso não exista aquela capacidade, a solicitação deverá ser endereçada ao Chefe das Operações (CO) que em coordenação com o coordenador de pesquisa (C) verificam se têm sensores adequados para obter esta informação e efetuam os pedidos aos diferentes sensores. Finalmente o Information Manager garante que a informação obtida é publicada nos locais adequados para que esteja disponível quando necessária.

CONCLUSÕES

As operações de GE e ISTAR contribuem ativamente e de forma individualizada para acelerar o Operational Planning Process (OPP) e integram o Conceito de Operações (CONOPS) e o Plano de Operações (PO). As duas actividades contribuem para o desenvolvimento do Intelligence Collection Plan (ICP).
Na NATO, a atividade principal de GE é coordenada pelo SEWOC (SIGINT and EW Operation Center), quando activado, o qual tem a responsabilidade de coordenar a actividade de GE com as áreas de Operações de Informação (InfoOps), gestão do espectro electromagnético, guerra da navegação, Informações, Vigilância e Reconhecimento.
A GE, isoladamente, ou através do SEWOC, participa no processo de atribuição de tarefas, no planeamento e na aquisição de objetivos, para assegurar que, com base nos requisitos de GE, os sinais relevantes no âmbito do ambiente eletromagnético sejam integrados na lista de tarefas de pesquisa ISR. Assim a atividade ISTAR apenas recebe contributos e exige coordenação no âmbito da GE na componente de vigilância eletrónica, baseando-se nas medidas de apoio eletrónico e nas Signal Intelligence (SIGINT), como fontes essenciais para fornecer Informações e apoiar na compreensão da situação operacional.
Para finalizar podemos referir que a GE é uma actividade independente, que exige estreita coordenação com outras actividades operacionais no âmbito do planeamento, contribuindo significativamente para aumentar a eficácia do processo de decisão.

Guerra Eletrónica: Evolução de Conceitos na NATO



Ten Tm (Eng.) Luís Dias

Introdução

A dependência do espectro eletromagnético durante as operações militares, "levou" a NATO (North Atlantic Treaty Organization) a definir o conceito de "Electromagnetic Environment" (EME). O EME é um Ambiente Operacional geofísico que conecta todos os outros domínios físicos como a Terra, o Ar, o Mar e o Espaço, realizando a "ponte" entre o Ambiente da Informação e estes domínios físicos. Assim, passa também a ser um lugar onde decorrem operações militares e onde se atingem os efeitos pretendidos.

A crescente evolução tecnológica dos sistemas de informação e dos sistemas de armas, assim como a crescente exploração do EME pelos adversários implica um aumento do esforço quer na perceção das consequências do uso da GE, quer no planeamento das ações de GE.

O foco da GE deixou de estar apenas no Espectro Eletromagnético (Electromagnetic Spectrum - EMS), para passar a estar centrado na conduta de "Electromagnetic Operations" (EMO) no EME.

As transformações num Ambiente Operacional tecnologicamente moderno continuam a crescer em complexidade, trazendo inúmeras oportunidades mas também vulnerabilidades. Assim, numa época em que o número de baixas e os danos colaterais são mais importantes que nunca, a GE assume um papel de relevo, podendo, de acordo com as regras de empenhamento, atuar onde outras armas não podem.

Novos Conceitos

A nova designação de Guerra Eletrónica traduz-se como a ação militar que explora a energia do EMS para fornecer a perceção da situação operacional (situational awareness) e conseguir efeitos ofensivos e defensivos.

A GE conduz EMO dentro do EME.

As EMO são todas as capacidades operacionais que dependem da utilização ou exploração do EMS. Como exemplos de EMO temos as comunicações, sensores (imagem, vigilância, reconhecimento e radares), outras formas de recolha de informações, a Guerra Eletrónica, aquisição de alvos e algum tipo de armamento. A GE é a vertente de Combate dentro das EMO.

As ações de GE são designadas de Electronic Attack (EA), Electronic Defence (ED), e Electronic Surveillance (ES).

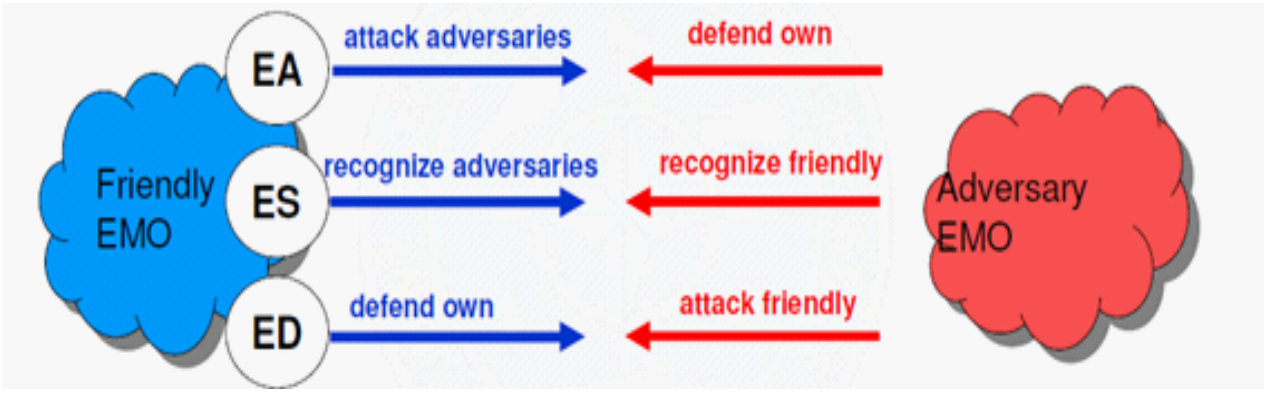


Figura 1 – Esquema representativo das Ações de GE.

Electronic Atack – Utilização da Energia Eletromagnética com finalidade ofensiva. Inclui armas de energia dirigida.

Electronic Defense – Utilização da Energia Eletromagnética para proteção (da força, área e plataforma) e assegurar o uso efetivo do EMS pelas nossas forças.

Eletronic Surveillance – Utilização da Energia Eletromagnética para perceção da situação operacional e recolha de informações.

Medidas da GE

As medidas de GE são os mecanismos através dos quais se conseguem implementar as ações de GE, sendo utilizadas e planeadas pelos especialistas em GE. Na prática destinam-se ao planeamento tático e à execução, podendo dizer-se que são as "ferramentas" da GE.

Electronic Counter Measures (ECM) – medidas para impedir ou reduzir o uso efetivo do EMS pelo adversário através do uso de Energia Eletromagnética. Inclui Empastelamento, Deceção Eletrónica e Neutralização Eletrónica.

Eletronic Protetive Measures (EPM) – medidas para assegurar o uso efetivo do EMS pelas nossas forças apesar do uso de Energia Eletromagnética pelo adversário. Dividem-se em Medidas Ativas (detetáveis pelo adversário) e Medidas Passivas (não detetáveis pelo adversário).
Electronic Warfare Support Measures (ESM) – medidas para realizar pesquisa, interceção e identificação de emissões eletromagnéticas e localizar as fontes com o propósito de localizar ameaças.

Relação entre Ações e Medidas de GE

O quadro seguinte espelha as relações entre todas as variáveis relativas à GE presentes no Ambiente Eletromagnético.

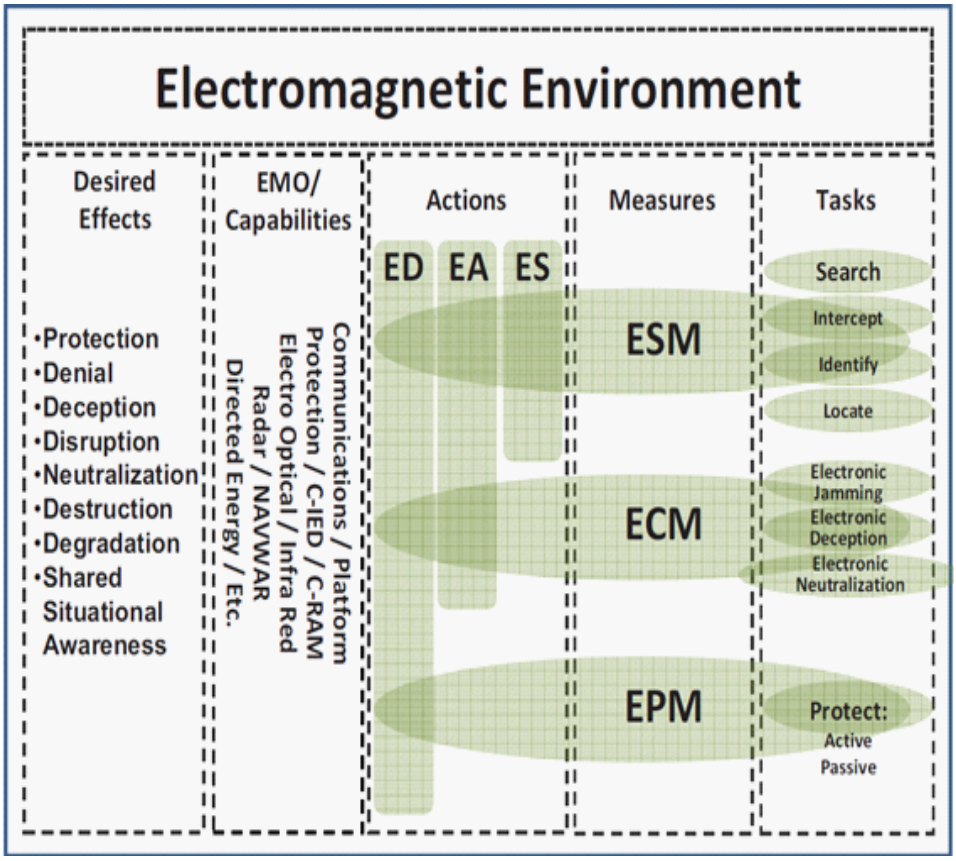


Figura 2 – Relações entre as operações de GE.[1]

Como se verifica, para obter diversos efeitos (Proteção, Destruição, Deceção, etc.), a GE atua nas capacidades militares que decorrem através de EMO (Comunicações, C-IED, Radar, etc.). A GE pode atacar, defender e vigiar dentro do Ambiente Eletromagnético, materializando essas ações através de medidas (ESM,ECM,EPM) que contemplam diversas tarefas específicas. Para que tudo se torne mais claro, seguem-se alguns exemplos.

1 NATO STANDARTIZATION AGENCY (2011), ALLIED JOINT DOCTRINE FPR ELECTRONIC WARFARE, AJP3.6 (B)

Exemplos de Ações de GE

Eletronic Surveillance:



Figura 3 – Atuação das Light Electronic Warfare Team.

Na figura acima encontra-se o cenário típico das denominadas Light Electronic Warfare Team (LEWT) pertencentes aos Royal Corps of Signals de Inglaterra, em atuação no Afeganistão desde 2009. A LEWT é integrada numa patrulha de infantaria e é composta por um operador de GE e um intérprete. O operador tem a tarefa de intercetar e localizar comunicações inimigas, descodificadas pelo intérprete (Afegão), analisadas e transmitidas de imediato para o comandante da patrulha e para a retaguarda via TacSat[1] .
Relatos de militares ingleses afirmam que as LEWT já salvaram vidas, identificando a direção do inimigo em situações de emboscada, realçando que de outra forma teria sido fatal.
Este é um cenário típico de uma ação de ES com a finalidade de obter uma perceção da situação tática. Para operacionalizar a ação de ES empregam-se as diversas tarefas das ESM. A guerra no Iraque (1991), com nome de código “Desert Storm”, teve o seu início com operações aéreas.

1 Rádio para comunicações táticas em UHF via Satélite.

Electronic Atack:



Figura 4 – Meios Aéreos VS Defesa Anti Aérea, na operação “Desert Storm”.

A GE foi uma das componentes mais presentes no início destas operações para destruição do avançado sistema de defesa área do Iraque (designado de “KARI”). Um dos primeiros objetivos da coligação era a destruição dos centros de comunicações chave para o sistema KARI, cujo funcionamento era em rede através de ligações de feixes.
Uma das medidas adotadas foi empastelar os sistemas de comunicações do KARI, colocando o processo de decisão do sistema inoperacional. De seguida, através de engodos (chaff – palhetas de alumínio refletoras) conseguiu-se a ativação dos sistemas de radares, sendo possível a destruição dos mesmos com recurso a mísseis HARM (High speed anti radiation missile).
Em suma, após o levantamento do funcionamento e das vulnerabilidades do sistema “KARI”, a coligação desenvolveu um plano detalhado e em poucas horas destruiu o então avançado sistema de defesa aérea.
Assim, pode constatar-se que estamos perante um EA planeado pela coligação, com recurso a aeronaves com capacidades de Guerra Eletrónica para destruir o sistema de defesa aérea inimigo. As ESM foram utilizadas no levantamento da ordem de batalha eletrónica do sistema KARI e na aquisição de alvos aquando o lançamento dos mísseis HARM. As ECM foram aplicadas no empastelamento dos sistemas de comunicações e na deceção (lançamento de chaff) aos radares Iraquianos. Electronic Defense:
Percebendo os exemplos anteriores, é muito simples pensar numa operação de ED. A ED visa defendermo-nos de EA inimigos. Assim todas as medidas da GE são transversais a esta ação.



Electronic Defense:
Percebendo os exemplos anteriores, é muito simples pensar numa operação de ED. A ED visa defendermo-nos de EA inimigos. Assim todas as medidas da GE são transversais a esta ação. Como exemplo, na proteção das plataformas (aeronaves, navios e cada vez mais de carros de combate) contra armas guiadas por RF, IR ou Laser, é desencadeada uma operação de ED, sendo o primeiro alerta dado pelas ESM que atuam como sensores de ameaças, enviam esta informação aos sistemas de ECM, que por sua vez atuam os sistemas de deceção adequados (flares, chaff, etc).
Entre vários exemplos de operações de ED destaco a Batalha Naval de Lataquia entre forças de Israel e da Síria. Em resumo, a capacidade de GE Israelita revelou-se fulcral contra os misseis guiados de longo alcance dos Navios da Síria.
Também como exemplos de ED destacam-se os sistemas de proteção de força, nomeadamente o uso de inibidores de frequência contra ativação de engenhos explosivos por controlo remoto.
Por fim, as EPM são intrínsecas à ação de ED e devem ser transversais a todas as capacidades operacionais do ambiente eletromagnético. Entre várias EPM destaco: a mudança de frequência (método ineficaz face aos sistemas de empastelamento mais avançados), parâmetros da transmissão mais imunes a EA (Frequency hoping, Spread Spectrum, etc.), uso de antenas direcionais (de modo a evitar interceção pelo adversário), procedimentos rádio, uso restrito à real necessidade, potência necessária, etc.

Conclusões

Neste artigo abordaram-se alguns dos novos conceitos operacionais de GE ao nível NATO. A alteração recente dos conceitos de Guerra Eletrónica, tanto ao nível do emprego operacional como das medidas de coordenação[1] necessárias em operações conjuntas da NATO, são reveladoras da importância que é dada a esta matéria.
Foram focados exemplos práticos de utilização de GE, e como vimos, a GE é muito mais para além de um sensor do campo de batalha. Estende-se também ao ataque e proteção no Ambiente Eletromagnético com efeitos que são repercutidos em todos os domínios físicos.
A evolução tecnológica assume um ritmo vertiginoso, e a dependência tecnológica quer da população civil, das forças militares, de forças inimigas, terroristas e insurgentes, tornam claro que para a GE atuar com sucesso, a coordenação é fundamental para assegurar a utilização eficiente e eficaz das medidas de GE.
A fronteira ténue, entre os efeitos produzidos por determinadas ações de Guerra Eletrónica e algumas das designadas Computer Network Operations, as "armas" da Guerra do Comando e Controlo, revelam uma necessidade cada vez maior de trabalho conjunto e sincronizado. Exemplo desta complementaridade é a semelhança entre o efeito obtido pela ação de empastelar (GE) um sistema de comunicações ou efetuar um ataque do tipo Denial of Service[2] (CNO). Outro exemplo é a evolução de armas de jamming (empastelamento) com capacidades de atuação "inteligente", ou seja, extrapolando a barreira dos sinais para os dados contidos no sinal.
Por fim, sabendo que os potenciais adversários sabem da enorme dependência das operações militares no EME, a NATO considera este um campo de batalha promissor e com altas probabilidades de ser atacado pelos adversários.

Bibliografia:

Tucker, S. (2010), "The Encyclopedia of Middle East Wars: The United States in the Persian Gulf, Afghanistan, and Iraq Conflicts". California: ABC-CLIO.
NATO STANDARTIZATION AGENCY (2011), "ALLIED JOINT DOCTRINE FOR ELECTRONIC WARFARE, AJP3.6 (B)".
Scott A., Hardy T., Martin R., Thomas R.(2011), "What are the Roles of Electronic and Cyber Warfare in Cognitive Radio Security?". USA: The Air Force Institute of Technology.

1 Não foram alvo de estudo neste artigo.

2 Tornar um recurso de uma rede de computadores, tal como um servidor Web, inacessível.

Sistema de Radiolocalização de Emissões Eletromagnéticas (SRE2)





Ten Tm (Eng.) Martingo Coelho

Fig. 1 – Sistema de Radiolocalização de Emissões Eletromagnéticas (SRE2)

1 - Introdução

A Companhia de Guerra Eletrónica dispõe atualmente de seis estações móveis dedicadas de azimutagem de emissões eletromagnéticas. Para se realizar uma radiolocalização são necessárias pelo menos três estações posicionadas em locais distintos e simultaneamente um sistema de informação que permita efetuar a recolha dos dados de cada estação e posterior análise dos dados obtidos. Esta última permite, através da interceção dos dados de azimutagem, determinar a posição estimada da respetiva emissão eletromagnética, esquematizada na figura 2.

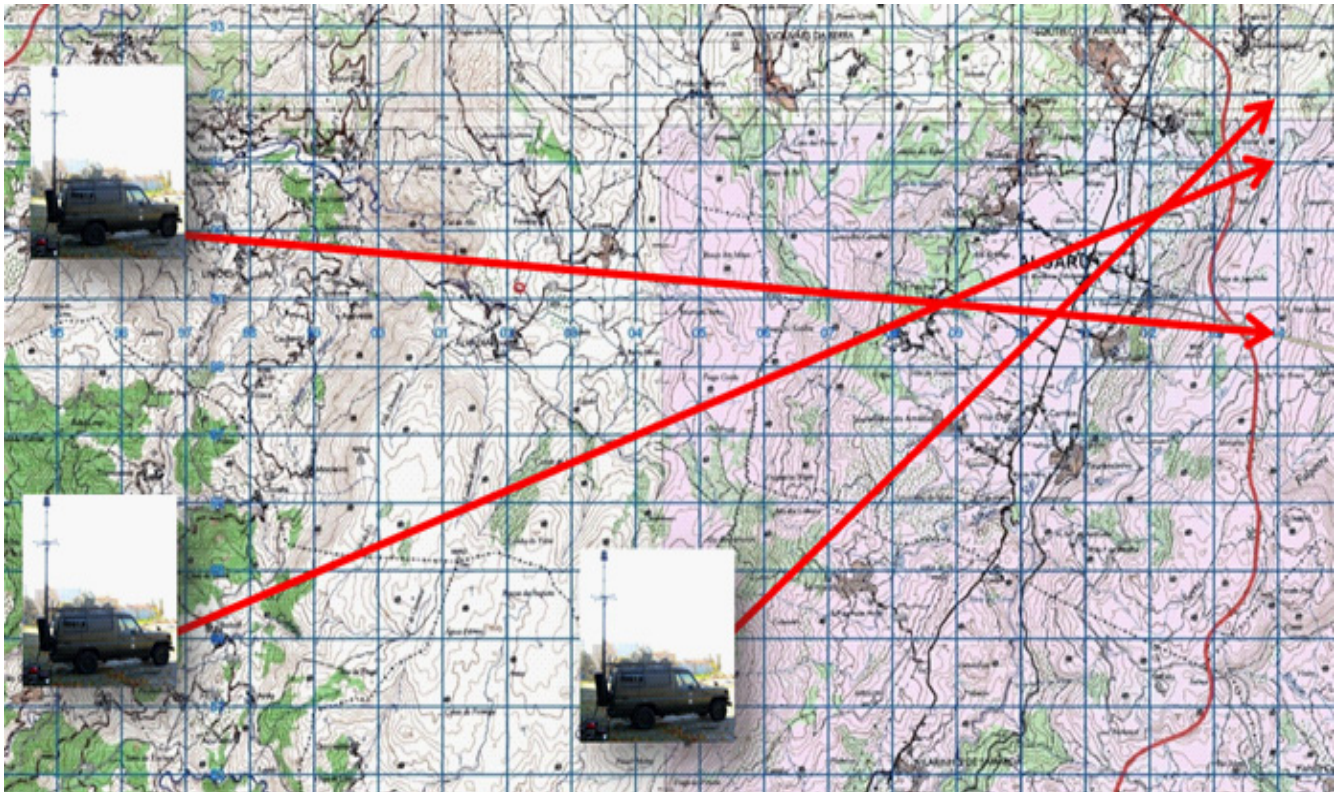


Fig. 2 - Radiolocalização

2 - Funcionamento e limitações atuais

Atualmente, as secções de radiolocalização, cada uma constituída por 3 equipas de radiolocalização, executam o seu trabalho de uma forma antiquada e pouco eficiente.
Ao chegar ao local estabelecido para executar a sua missão, cada equipa tem que orientar (manualmente) a antena do equipamento para Norte, com o auxílio de uma bússola magnética tradicional (e.g. Bússola Silva). Qualquer erro na orientação da antena do equipamento de DF (Direction Finding) irá refletir-se no valor do azimute obtido para uma determinada emissão eletromagnética e, consequentemente, traduzir-se num erro de radiolocalização. Outra informação essencial para a radiolocalização é a posição geográfica das equipas, uma vez que os azimutes são traçados a partir dessas posições. As equipas registam as suas coordenadas através de cartas topográficas militares com o auxílio de um escalímetro.
Após detetarem uma emissão eletromagnética e registarem os dados dessa emissão, as equipas comunicam-nas ao seu comandante de secção de radiolocalização, para que este possa determinar a posição estimada da respetiva emissão eletromagnética. Esta comunicação é atualmente efetuada à voz através do E/R PRC-425.
Este tipo de funcionamento acarreta vários inconvenientes:
- Grande probabilidade de erro: originado principalmente pelo “erro humano” inerente às tarefas manuais a concretizar pelas equipas, desde a orientação da antena até às coordenadas da própria posição geográfica;
- Processo muito demorado: poderá por em causa o sucesso de missões onde o tempo de atuação é escasso;
- Falha de segurança: as comunicações entre as equipas são feitas em claro expondo a missão à Guerra Eletrónica adversária.

3 - Organização do SRE2

O SRE2 é um sistema projetado para colmatar as limitações anteriormente referidas, através da integração de vários equipamentos: GPS, bússola eletrónica, equipamento de DF (PA1100) e equipamento rádio (VRC 525HV). O sistema está organizado em dois subsistemas, em que um deles é dedicado às equipas de radiolocalização (Slave) e o outro ao comandante da secção de radiolocalização (Master), esquematizado na figura 3. O SRE2 utiliza uma aplicação "GE_Application" que foi desenvolvida na Companhia de Guerra Eletrónica pelo Tenente André Calvinho.

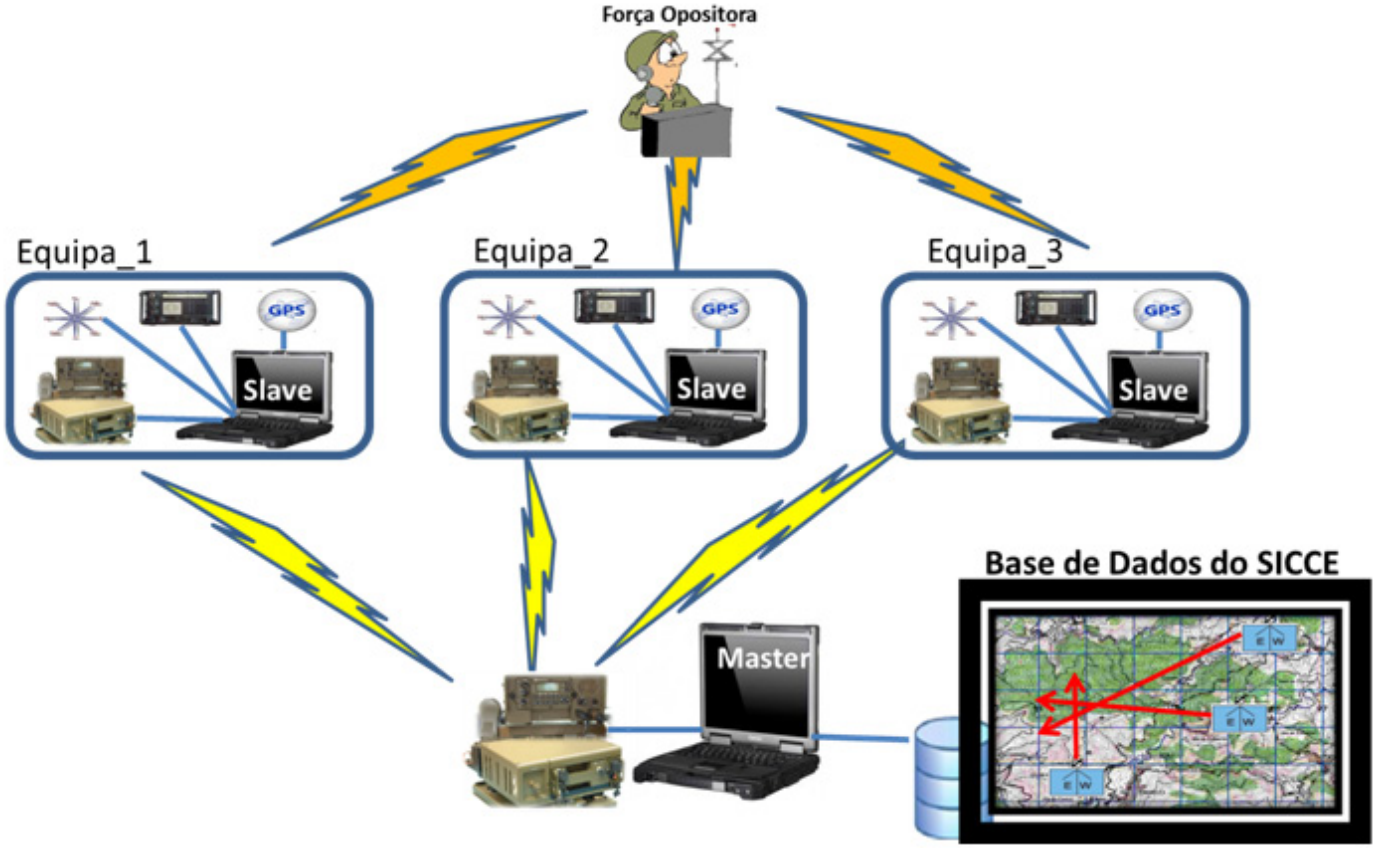


Fig. 3 – Estrutura do SRE2

3.1 – Subsistema de Equipa de Radiolocalização (Slave)

O subsistema de equipa de Radiolocalização é constituído por um GPS, uma bússola eletrónica, um equipamento de DF (PA1100), uma montagem veicular VRC 525HV, um computador portátil e respetivo sistema de alimentação, figura 4.

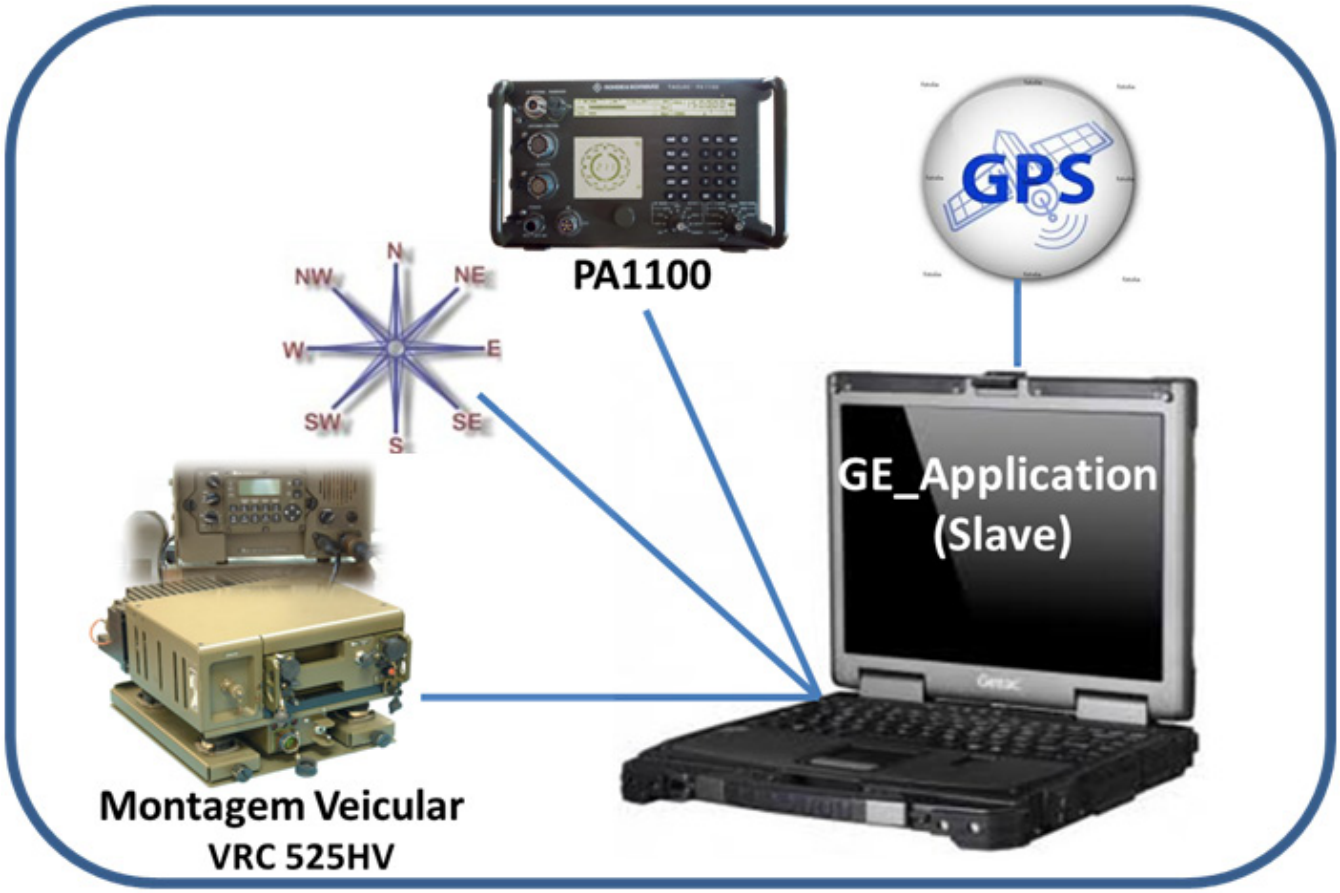


Fig. 4 – Subsistema de Equipa (Slave)

Os diversos equipamentos serão interligados ao computador através de um adaptador USB<-> 4×Rs232. O computador terá instalado a aplicação "GE_Application_Slave", que será responsável pela integração dos vários equipamentos no subsistema.

O SRE2 vai permitir uma automatização dos procedimentos de instalação e operação dos meios por parte da equipa de radiolocalização. O GPS enviará para a aplicação a posição atual da equipa em tempo real, retirando a necessidade que a equipa tinha de se georreferenciar com base nas cartas militares e escalímetro. Os dados enviados pela bússola eletrónica vão anular a necessidade da orientação manual da antena de DF para norte, sendo que a aplicação fará automaticamente o acerto dos azimutes obtidos. A aplicação também permitirá o envio ou receção de dados entre a equipa e o seu comandante de secção, através da montagem veicular VRC 525HV de forma segura (utilização de cifra e/ou salto em frequência).

3.2 – Subsistema de Comando (Master)

O subsistema de comando é constituído simplesmente por um computador interligado a uma montagem veicular VRC 525HV. Neste computador, estará instalada a aplicação "GE_Application_Master" que através de uma interface gráfica própria permitirá a troca de dados seguros, entre o comandante da secção de radiolocalização e as suas equipas, através do rádio 525HV, figura 5.



Fig. 5 – Subsistema de Comando (Master)

Este computador deverá ainda conter uma aplicação que permita introduzir os dados obtidos pelas equipas, numa base de dados, possibilitando dessa forma que outras aplicações possam efetuar a triangulação dos registos obtidos, para obtenção da posição geográfica da emissão eletromagnética em causa. Para esse efeito poderá ser utilizado o SICCE (Sistema de Informação para o Comando e Controlo do Exército) de duas formas distintas: localmente na própria máquina ou remotamente através de uma ligação TCP/IP. Para a interligação entre a GE_Application e o SICCE é necessário recorrer a uma outra aplicação denominada de Servidor de Ligações ao SICCE, desenvolvida pelos Capitães Pedro Fernandes e João Fernandes em 2007.

3.3 - Esquema da Montagem Veicular VRC 525HV

A montagem veicular projetada para o SRE2 utiliza o rádio 525HV que permite comunicações de voz e dados em HF e VHF de forma segura (utilização de cifra e/ou salto em frequência).

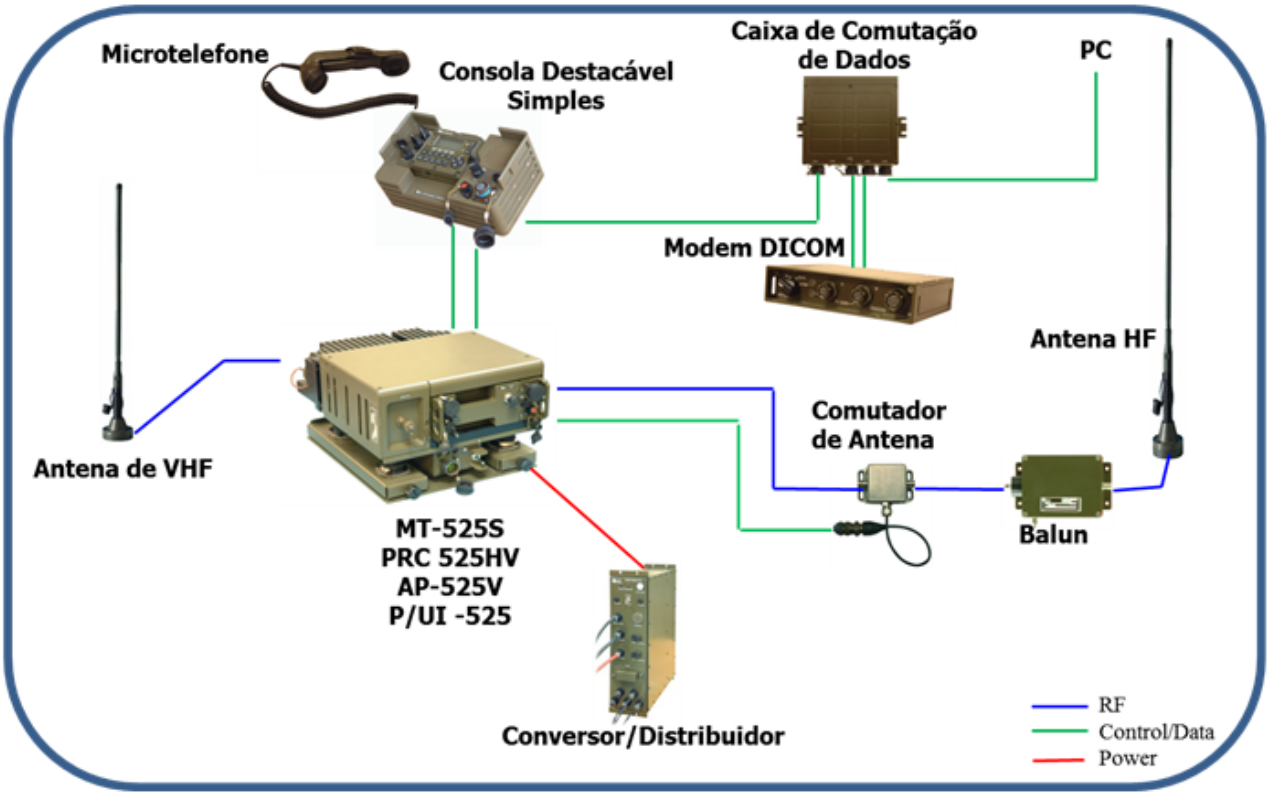


Fig. 6 – Montagem veicular VRC 525HV

A montagem, figura 6, será alimentada a 24 V DC pelo conversor/distribuidor a partir do sistema de alimentação. Será utilizado o suporte mecânico MT-525S para instalação do PRC 525HV e amplificador de potência, que fornece também comutações adicionais HF/VHF ao sistema. A consola destacável simples comporta o altifalante e suporta o painel frontal do rádio, permitindo o controlo remoto do radio e interconexão com o computador. A caixa de comutação de dados simples efetua a comutação entre os diversos tipos de dados a utilizar na comunicação (Modem interno-rádio, Modem externo, FSK, Fill Gun). A aplicação "GE_Application" utilizará o modem interno-rádio em SECOM H, SECOM V ou OFDM, para enviar e receber dados.
Por motivos de segurança não são apresentados alguns detalhes da montagem veicular projetada.

3.4 - Esquema de Alimentação do SRE2

A alimentação do SRE2, esquematizada na figura 7, foi projetada de modo a aproveitar os equipamentos de alimentação já existentes, de forma a reduzir os custos de implementação. O sistema atual contempla um gerador de 230 V AC, um carregador/inversor 230 V AC <-> 12V DC e duas baterias de 12 V, possibilitando pontos de alimentação de 230 V AC e 12 V DC. Para o SRE2, além dos pontos de alimentação existentes, é necessário também um ponto de alimentação de 24 V DC para alimentação da montagem veicular VRC525HV projetada. Assim sendo, será incrementado no sistema atual um conversor/distribuidor 230 V AC para 24 V DC, devidamente dimensionado para a potência necessária da montagem veicular.

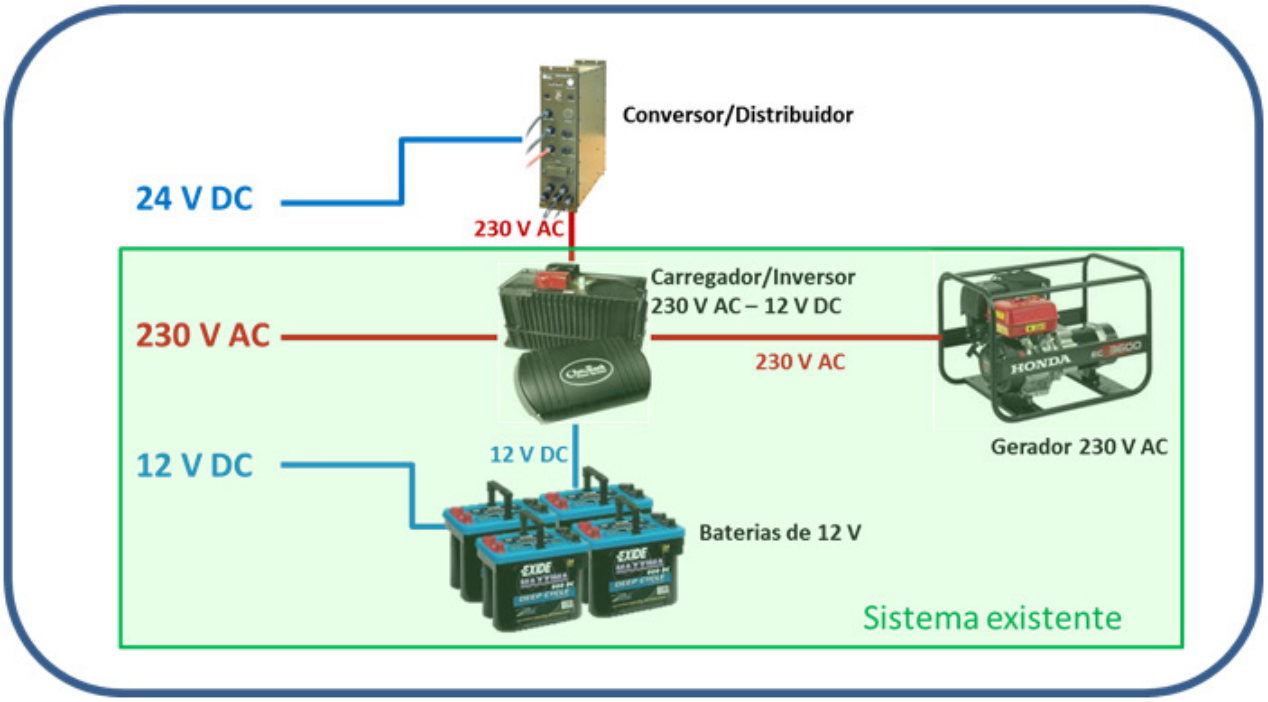


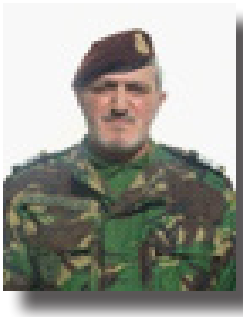
Fig. 7 - Esquema de alimentação do SRE2

4 – Conclusões

O SRE2 vai permitir a automatização de alguns dos procedimentos de instalação e operação dos meios por parte das equipas de radiolocalização. O tempo necessário para a instalação e comunicação de dados vai ser menor, podendo ser determinante para o sucesso de missões onde o fator tempo seja crítico.
O facto de o SRE2 utilizar a montagem veicular VRC 525HV com amplificação vai permitir manter a ligação entre as equipas a maiores distâncias, conferindo uma área de atuação superior. O rádio 525 vai possibilitar comunicações de voz e dados de forma segura, através da utilização de salto em frequência e/ou utilização de cifra.
A implementação do SRE2 vai proporcionar uma diminuição da probabilidade de erro nos resultados da radiolocalização, uma vez que eliminará possíveis erros na orientação manual da antena e erros nas coordenadas das posições geográficas das equipas.
O SRE2 permite, ainda, a ligação ao SICCE de forma a registar e permitir um comando e controlo centralizado das atividades realizadas.

Colaboração da Escola Prática de Transmissões com as Autoridades e Entidades Civis e Militares

Pela sua missão, localização geográfica específica - inserida na malha urbana da cidade do Porto - e ainda pelo significativo número de Quadros e de Praças, a Escola Prática de Transmissões tem potencialidades para se constituir como pólo de excelência na dinamização e divulgação da imagem do Exército. Desta forma, e no intuito de estreitar o contacto com a população e sensibilizar a comunidade civil para a Instituição Militar, a EPT tem acolhido ao longo do ano visitas de várias Escolas e outras Entidades Civis e Militares e prestado Apoio Logístico a Entidades Regionais e a outros Organismos.



TCor TExplTm Fernando Lobão

<u>Apoio Recreativo e Cultural</u>

Visitas à Unidade







Durante 2011 fomos visitados por cerca de oitocentos Jovens, com idades compreendidas entre os 7 e os 21 anos, pertencentes a treze Estabelecimentos de Ensino do Distrito do Porto.
Estas visitas tiveram a duração de um ou meio dia normal de serviço, conforme as solicitações, para as quais foram preparados programas ajustados quer à faixa etária dos visitantes, quer às exigências curriculares dos programas de ensino.

Colaboração da Escola Prática de Transmissões com as Autoridades e Entidades Civis e Militares

Programa "24 Horas no Exército"








Através das Escolas e das Associações de Pais, a Escola Prática de Transmissões tem vindo a proporcionar aos Jovens, dos 14 aos 17 anos, a possibilidade de passarem "24 Horas no Exército". Este programa tem por objetivo facultar aos Jovens uma estadia de um dia em ambiente Militar, proporcionando-lhes um leque alargado de atividades, tomando conhecimento da realidade Militar e dos Valores e Símbolos Nacionais.
Durante 2011 aderiram a este programa dois Estabelecimentos de Ensino do Distrito do Porto com oitenta e cinco Jovens e um Estabelecimento de Ensino do Distrito de Braga com quinze Jovens.

Cerimónias Diversas





Colaboração da Escola Prática de Transmissões com as Autoridades e Entidades Civis e Militares

A EPT acolheu várias solicitações para a realização na Unidade de Encontros Convívio de Ex-Combatentes e Cerimónias Militares de Homenagem aos Militares Mortos em Combate pela Pátria.
Estas cerimónias permitem manter a ligação entre os Ex-Combatentes e os seus familiares com os Militares que ainda se mantêm na efetividade de serviço.

Apoio Logístico

Alimentação e Alojamento







Foram alojados na Unidade cerca de dois mil Jovens que participaram no projeto “Universidade Júnior – Cursos de Verão 2011” promovido pela Universidade do Porto
A participação neste projeto, embora de forma indireta, tem permitido que milhares de Jovens, no período das suas férias de verão, contactem com os diversos Departamentos da Universidade do Porto, enriquecendo de forma categórica os Jovens que os visitam.
Foram ainda alojados na Unidade cerca de duzentos e cinquenta Jovens que participaram no projeto “Danone Nations Cup” que decorreu no estádio Jorge Sampaio em Vila Nova de Gaia.

A certificação como valorização da carreira técnica do Sargento de Transmissões



SMor Carlos Morais

O século que findou certamente será lembrado como um período de grande desenvolvimento tecnológico. A isto não ficou indiferente a União Europeia que assumiu o compromisso da sociedade do conhecimento para o seu espaço geográfico. Na realidade, até ao início do século passado o saber ler e interpretar textos e o efetuar cálculos matemáticos simples era obrigatório para se viver em harmonia e bem-estar na sociedade. O cenário mudou e as necessidades de qualificações profissionais e académicas aumentaram consideravelmente. O cidadão, pela obrigação de acompanhar este grau de exigência, tem vindo a adaptar-se a este novo paradigma da sociedade.

As ciências do saber adotam como prioridade a formação especializada dos cidadãos incutindo-lhes espírito empreendedor e criativo de grande capacidade para a resolução de problemas. Assim, o conceito de "formação profissional" surge como o processo através do qual os cidadãos adquirem e desenvolvem capacidades e competências, harmonizadas ao seu desempenho e valorização, profissional e pessoal, atualizando os conhecimentos detidos no exercício da sua atividade.
É precisamente em torno desta aquisição de conhecimentos e respetiva certificação que se desenvolve este texto, elencando-se contributos, ainda que exíguos, para a valorização da carreira do Sargento da Arma de Transmissões.

A carreira do Sargento de Transmissões do Século XXI

Ao Sargento de Transmissões, nos últimos 20 anos, tem-lhe sido exigidas qualificações e saberes técnicos e tecnológicos que acabam por lhe conceder um papel indispensável no cumprimento da missão destinada à Arma de Transmissões. A sociedade evoluiu e o Sargento de Transmissões acompanhou o progresso, adquirindo competências técnicas para o desempenho de funções de responsabilidade superior. Hoje, o acesso á carreira é feito com a conclusão do Curso de Formação de Sargentos (CFS), de duração de dois anos, complementado com o respetivo estágio de especialização, onde para admissão é exigido o 12.º ano de escolaridade com a aprovação na disciplina de Matemática.

Após a formação inicial, com uma componente horária superior a 3000 horas, a carreira formativa do Sargento de Transmissões progride ao longo dos anos de serviço, em formação contínua, direcionada para saberes técnicos e tecnológicos, na componentes do saber – fazer. Por outro lado, todo o percurso formativo, mas também escolar, é satisfeito de um amplo programa de acções de formação e informação, treino e qualificações de média duração, conferindo à formação desta categoria militar equidade com a que é ministrada, para outras categorias técnico profissionais idênticas, em estabelecimentos do ensino nacional.
Fazendo uma análise genérica aos aspetos técnico-formativos de toda a carreira, o caminho tende na credibilização e valorização profissional desta classe militar, quer inicialmente pela certificação das competências, quer numa segunda fase, na equivalência ao grau académico que as aptidões correspondam. Com toda a justiça, esta via valoriza uma carreira que decorre sempre na procura do saber, pela formação contínua.
A certificação profissional representa uma prova credível das competências profissionais adquiridas, reflectindo-se também no desenvolvimento mais adequado ao projecto pessoal de carreira e de valorização profissional de cada militar. Desta forma, para o Sargento de Transmissões, a atestação das suas aptidões é uma aspiração real e

legítima, e não pode parecer inacessível ou inatingível a quem se esforça e se empenha por isso. O reconhecimento da instituição militar e da sociedade civil deste desígnio é fundamental. A cultura de subvalorização da carreira de Sargento, existente na sociedade civil, tem de ser desmistificada, ganhando a instituição militar e o país. Na verdade quando se é, realmente, valorizado pela sociedade, o salário não é mais do que uma consequência natural disso mesmo.

A certificação profissional reconhecida no Estatuto dos Militares (EMFAR)

Presentemente, o Sargento de Transmissões distingue-se por uma carreira profissional, altamente técnica, de colaboração activa com a cadeia de comando em que se insere, tendo sempre presente o sentido do dever e o orgulho pela profissão que abraçou.
Admitindo a necessidade de formar militares do QP para uma "carreira altamente técnica", o legislador consagrou no EMFAR diverso articulado, como por exemplo o Artigo 79.º, que estabelece a certificação da profissão, "os cursos de formação ministrados nas Forças Armadas que confiram conhecimentos e aptidões habilitantes para o exercício profissional garantem o direito à respectiva certificação profissional". Inclusivamente, no acesso á carreira e após a respetiva formação inicial, certifica o 2º Sargento do QP com o nível III, conforme clarifica o Artigo 130.º, "para o ingresso na categoria de sargentos é exigido, no mínimo, o ensino secundário complementado por formação militar adequada ou formação militar que habilite com a certificação de formação profissional de nível 3".
Também no que concerne aos conteúdos formativos, ministrados nos estabelecimentos de ensino militar, o EMFAR no Artigo 71.º reconhece-os formalmente para habilitar os militares que os frequentam, com êxito, á correspondente equivalência com as escolas congéneres do processo educativo e formativo nacional.



A certificação é uma prova credível das competências profissionais adquiridas

A certificação das profissões por níveis

Desde 2008 que a legislação nos países da União Europeia, no âmbito da formação profissional e o respectivo reconhecimento de competências, está direcionada para certificar as profissões por níveis. Este princípio tem por objetivo a preparação dos quadros intermédios das organizações no desempenho de tarefas adquiridas pela experiência.

Neste contexto, o ingresso numa profissão com a habilitação do ensino secundário completo, complementada com a formação profissional geral e técnica, corresponde ao Nível IV. Esta capacidade profissional habilita o detentor a um trabalho técnico que pode ser executado de uma forma autónoma, incluindo responsabilidades de enquadramento e de coordenação.

A partir do nível IV, a perspetiva de carreira profissional passa, essencialmente, pela formação contínua. O acesso ao nível V faz-se com uma formação técnica pós-secundária, de alto nível, adquirida no âmbito das instituições escolares ou fora delas. A qualificação resultante desta formação inclui conhecimentos e capacidades que não exige, em geral, o domínio dos fundamentos científicos das áreas que integram a respetiva profissão, mas permitem assumir, de forma geralmente autónoma, responsabilidades de conceção e/ou de direção e/ou de gestão.

Por último, o acesso ao nível VI, faz-se por via da formação contínua, pós V nível, ou formação superior completa na área profissional. Esta formação conduz geralmente à autonomia no exercício da atividade profissional implicando o domínio dos fundamentos científicos da profissão. Essencialmente, procura-se valorizar ativamente as competências académicas, técnicas e profissionais dos cidadãos, incentivando a frequência de cursos de qualificação técnica. O nível VI, resultante da formação contínua, inclui conhecimentos que pertencem a um nível académico do ensino superior politécnico.



A aquisição de novas competências exige uma formação formal que se prolonga para lá do CFS

A certificação como valorização da carreira técnica do Sargento de Transmissões

O desenvolvimento da formação técnico-militar do Sargento de Transmissões

A Escola de Sargentos do Exército (ESE) tem a missão de qualificar os militares da categoria de Sargento. Aos da Arma de Transmissões denominados de Técnicos devido á especificidade da sua missão, especializa-os com apoio técnico-pedagógico e científico da Escola Prática de Transmissões (2º Ano/1º Semestre e estágio), do Centro Militar de Electrónica (2º Ano/2º Semestre e estágio) e do Regimento de Transmissões (estágio), nas áreas de Comutação e Redes (430-TCR), de Eletrónica e Equipamento Rádio (415-TEER) e na de Sistemas de Informação e Mensagens (424-TSIM).

Segundo o EMFAR, a certificação profissional está implícita com a conclusão do CFS nas respetivas especializações, correspondendo-lhe a qualificação do nível III. Não fazendo alusão aos níveis seguintes, estes devem ser reconhecidos, posteriormente, com a frequência e conclusão dos diversos cursos ministrados ao militar para acesso a graduação superior designadamente, o CPSA e o CPSCh, patamares finais de cada nível, consolidando também a progressão formativa e académica dos restantes cursos técnicos de aperfeiçoamento ou de qualificação frequentados até essas etapas.

Se, por um lado, a necessidade de aquisição de novas competências exige uma formação (e educação) formal que se prolonga para lá do CFS, por outro, o ritmo de evolução tecnológica conduz a que cada vez mais os técnicos militares vejam as suas competências rapidamente desatualizadas. Este antagonismo impõe ao Sargento de Transmissões o estabelecimento do fio condutor da sua especialização no plano dos valores, princípios, técnicas, direitos e deveres.

Nos últimos anos, da parte da instituição militar tem havido um esforço continuado na melhoria de métodos e conteúdos dos cursos técnico-militares. O saber-fazer tem sido a base da formação, no entanto, o saber-ser e o saber-estar são valores indispensáveis ao sucesso profissional do militar.



A admissão ao CFS é feita com o ensino secundário completo com a disciplina de Matemática do 12.º ano

A certificação como valorização da carreira técnica do Sargento de Transmissões

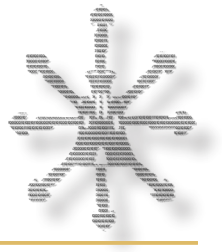
Voltando á progressão profissional por níveis e comparando-a com a restante sociedade, referenciando-a ao normativo do IEFP (Instituto do Emprego e Formação Profissional), entidade gestora do Sistema Nacional de Certificação Profissional, a formação contínua dos Sargentos de Transmissões até á patente de Sargento-ajudante equivale à frequência de um curso de especialização tecnológica, considerado pós-secundário de qualificação profissional de nível V. Esta classificação visará suprir as necessidades verificadas ao nível de quadros técnicos intermédios, respondendo aos desafios colocados por tarefas ou missões, em permanente mudança e acentuado desenvolvimento tecnológico, surgindo como uma alternativa válida para a profissionalização de técnicos especializados e competentes.

A formação ao longo da vida atingiria o topo, com o nível VI, após conclusão do CPSCh colocando, desta forma, os postos superiores de Sargento (SCh e SMor) no desempenho de funções de chefia e gestão de especificidade técnica. Paralelamente, e não menos importante, toda a carreira profissional militar deve ser reconhecida "universalmente", como composta de profissionais tecnicamente competentes no desempenho de tarefas idênticas às exigidas a outros profissionais de atividades técnicas análogas.



O Sargento de Transmissões adquirindo competências técnicas para o desempenho de funções superiores

A certificação como valorização da carreira técnica do Sargento de Transmissões



Revalorização dos recursos humanos

Em contexto de mudança, novas condições são exigidas às instituições e em todas está implícito, e por vezes explícito, um instrumento preponderante; - os recursos humanos, principal fonte do valor acrescentado para a eficácia dessa alteração. A revalorização dos recursos humanos passa pela criação de factores motivacionais, adaptados constantemente às necessidades destes e da inovação tecnológica.
As constantes transformações e a evolução do conhecimento técnico-científico constituem as bases da formação contínua. A experiência profissional é o suporte onde recaem as competências, reconhecidas ou não, e o nível de qualificação. No entanto, não reconhecer a importância deste capital individual, nem as possibilidades de ele ser identificado, avaliado, reconhecido, validado e certificado, equivale a uma desvalorização da vida face aos diplomas.
Numa época em que a gestão de competências está na ordem do dia, o sucesso das organizações depende das aptidões dos seus profissionais. Ao aumento de habilitações correspondem outras ambições a nível de progressão profissional e da própria gestão pessoal de uma carreira, permitindo outras soluções que não apenas a progressão vertical. Para o país, e evidentemente para a instituição militar, a certificação profissional deve representar o aumento da eficácia dos seus militares na resolução das tarefas que lhes são atribuídas, servindo também como fator motivacional.
Importa incutir nestes técnicos militares a consciência da necessidade de continuarem a desenvolver o seu capital de competências durante toda a carreira, não só como fator de estabilidade profissional, mas igualmente com a perspectiva de um novo caminho profissional numa área técnica da sociedade civil.
A qualificação escolar e profissional deve continuar a ser uma prioridade para a categoria do Sargento de Transmissões, pelo que se procurou com este documento fazer a caracterização formativa, de âmbito geral, de uma carreira que exige a constante actualização técnica, comparando-a com outras profissões de tecnicidade similar na sociedade civil.
Por último, com a existência cumulativa, mas dispersa, de três condições determinantes, designadamente, a legislação portuguesa, a aspiração dos militares e o interesse da instituição, julgam-se reunidas as condições para operacionalizar a ambicionada certificação profissional dos Sargentos de Transmissões.

Bibliografia:

- Área de Formação (Portaria n.º 256/2005, de 16 de Março).
- Castro, José Manuel, assistente convidado Faculdade Psicologia e Ciências da Educação da Universidade do Porto, “Formação e desenvolvimento tecnológico”, pp 42 a 44 Revista Dirigir, Jul/Set 2006.
- Certificação das profissões, in Instituto do Emprego e Formação Profissional (http://www.iefp.pt)
- Estatuto dos Militares das Forças Armadas (EMFAR), (Decreto-Lei n.º 236/99, de 25Jun, com as alterações e rectificações introduzidas pela Declaração de Rectificação n.º 10-BI/99, de 31Jul, Lei n.º 25/2000, de 23Ago, Decreto-Lei n.º 232/2001, de 25Ago, Decreto-Lei n.º 197-A/2003, de 30Ago, Decreto-Lei n.º 70/2005, de 17Mar, Decreto-Lei n.º 166/2005, de 23Set e Decreto- Lei n.º 310/2007, de 11 Set.)
- Normas provisórias de frequência, avaliação e classificação do CFS, a partir de 2004/2005, Despacho do Gen CEME, de 03Out03, com alterações produzidas pelos Despachos do Gen CEME de 25Jan05 e 21Abr05.
- “Sociedade da Informação”, Fundação Portugal Telecom (http://fundacao.telecom.pt).
- Tabela de Níveis de Formação, anexa à Decisão nº 85/368/CEE, do conselho, de 16 Julho, publicada no Jornal oficial das Comunidades Europeias nº L 199, de 31 de Julho - ao Despacho Normativo nº 4-A/2008, de 24 de Janeiro.
- Teixeira, Sebastião, Gestão das Organizações, pp 119, Mc-Graw Hill.



ALF TPO TIAGO SANTOS

1. INTRODUÇÃO

Desde sempre os sistemas de informação têm um papel fundamental nas sociedades e na defesa dos interesses nacionais. Está presente neste artigo o desenvolvimento de um sistema de vigilância não tripulado - UGV – Unmanned Ground Vehicle, destinado à obtenção remota de dados. Posteriormente e como complemento, será descrita uma aplicação para resposta a catástrofes com base nos sistemas remotamente controlados. A segurança de uma Nação também passa por sistemas capazes de responder a catástrofes naturais e humanas. Existe a possibilidade de usar este sistema em resposta e em prevenção destes incidentes.

2. DESENVOLVIMENTO DE UM UGV

Após alguma pesquisa, existem diversos requisitos para o desenvolvimento de veículos não tripulados militares [1]. Contudo, apenas se vai abordar o desenvolvimento deste sistema em relação ao software de controlo do UGV, a plataforma Surveyor SRV-1, figura 1. Esta é uma plataforma de navegação não tripulada de testes que permitirá posteriormente implementar outra de maiores dimensões. Contudo, nesta fase de desenvolvimento é a plataforma ideal uma vez que exige menos recursos devido às suas pequenas dimensões.



Figura 1 – Surveyor SRV-1

Com o intuito de reduzir o custo de desenvolvimento, optou-se por desenvolver o sistema com base numa plataforma e em software open – source, utilizando-se uma distribuição de Linux – Ubuntu e a linguagem de programação Python. Optou-se assim por uma linguagem de programação que permitiu um desenvolvimento mais rápido da aplicação, tendo-se ainda deixado a segurança das comunicações para uma fase posterior. Esta decisão prendeu-se essencialmente com o fato do equipamento disponível não possuir capacidade de processamento para todo o cálculo adicional relacionado com a criptografia. Na figura 2 apresenta-se um esquema do sistema em desenvolvimento.

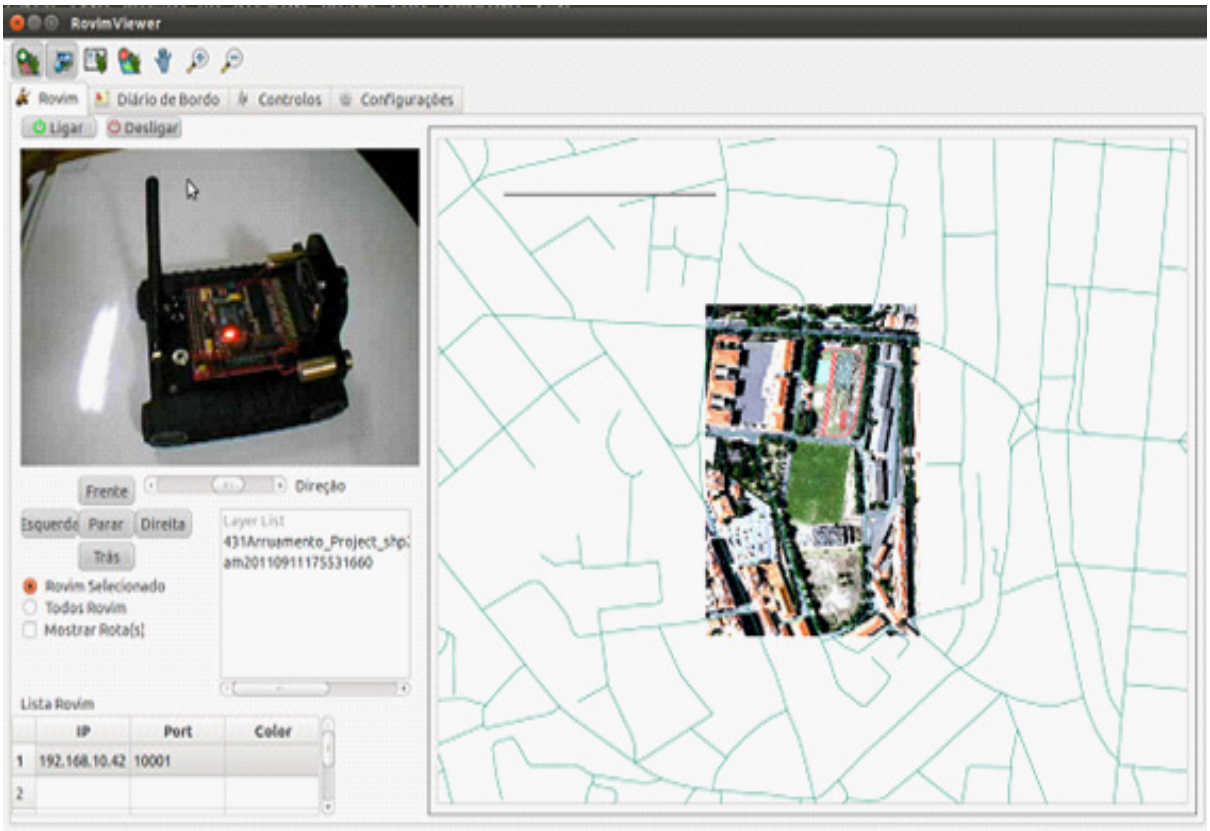


Figura 2 – RovimViewer – em testes

Do sistema desenvolvido fazem parte cinco módulos que, integrados, dão origem ao RovimViewer. Esses cinco módulos são:

1. Observação e monitorização – Visualização do meio envolvente, estado dinâmico e físico do UxV1[1], figura 3;

1 UxV – Unmanned x-environment Vehicle. Sistema desenvolvido para controlar qualquer tipo de sistema não tripulado desde que funcione por IP – Internet Protocol.

2. Sistema SIG – Disponibiliza informação geográfica e permite observar em tempo real a localização por intermédio de GPS – figura 4. Configuração e Controlo – Atribuição de teclas para controlar o UxV – figura 5;

3. Diário de Bordo e apresentação de mensagens assíncronas – Permite em caso de erro obter dados relativos ao problema detectado pelos sensores – figura 6;

4. Servidor de protocolo – Permite adaptar a aplicação a um novo sistema robótico;

5. Servidor de cálculo adicional – Permite prever a rota em caso de perda do sinal de GPS.

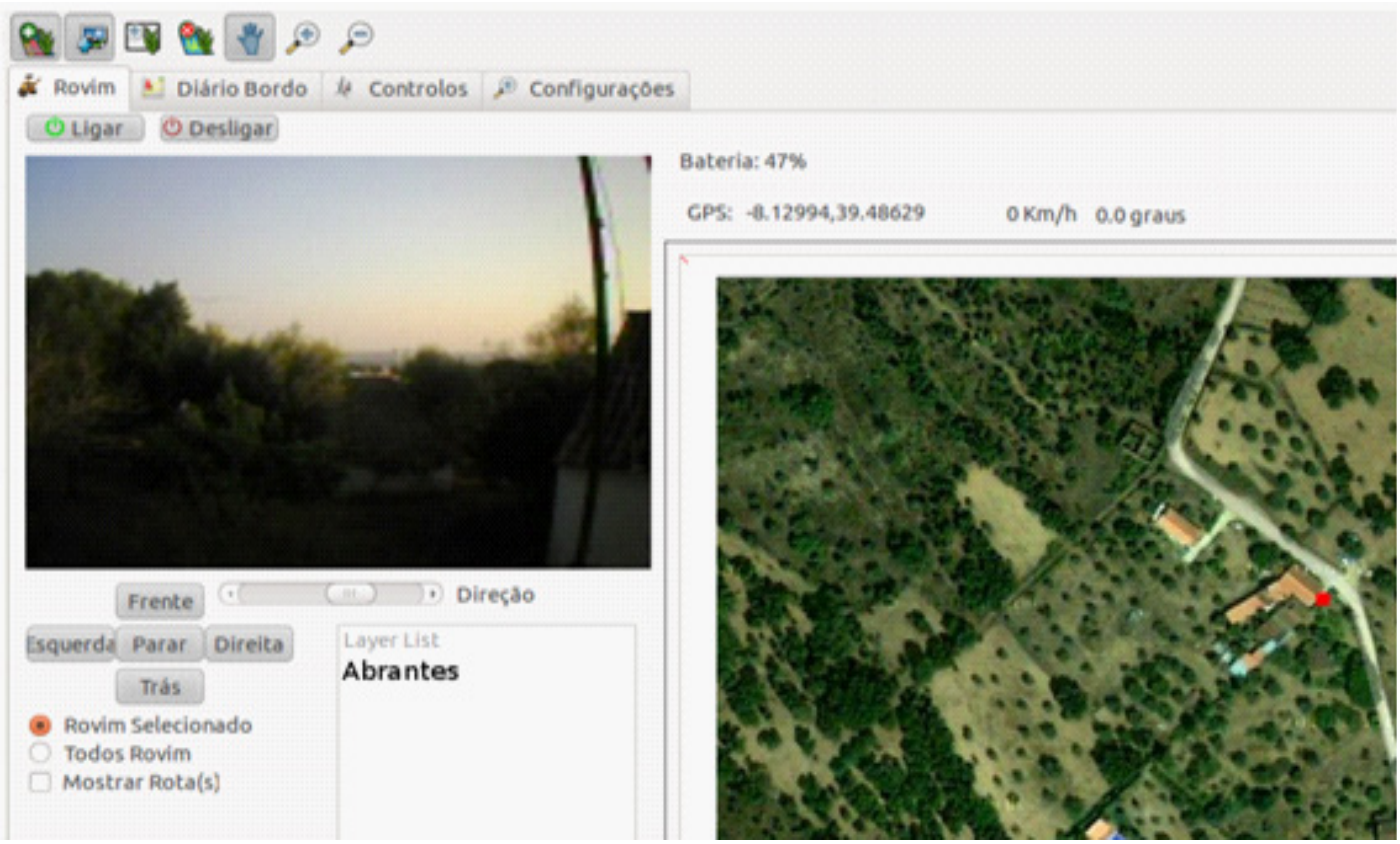


Figura 3 – Módulo de Observação e de Localização GPS.

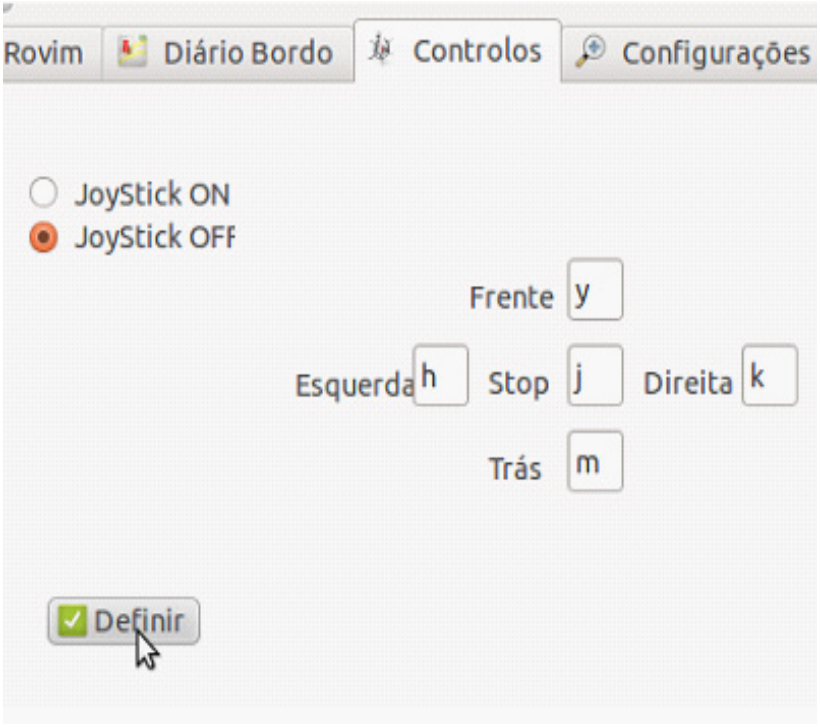


Figura 4 – Módulo da configuração das teclas.

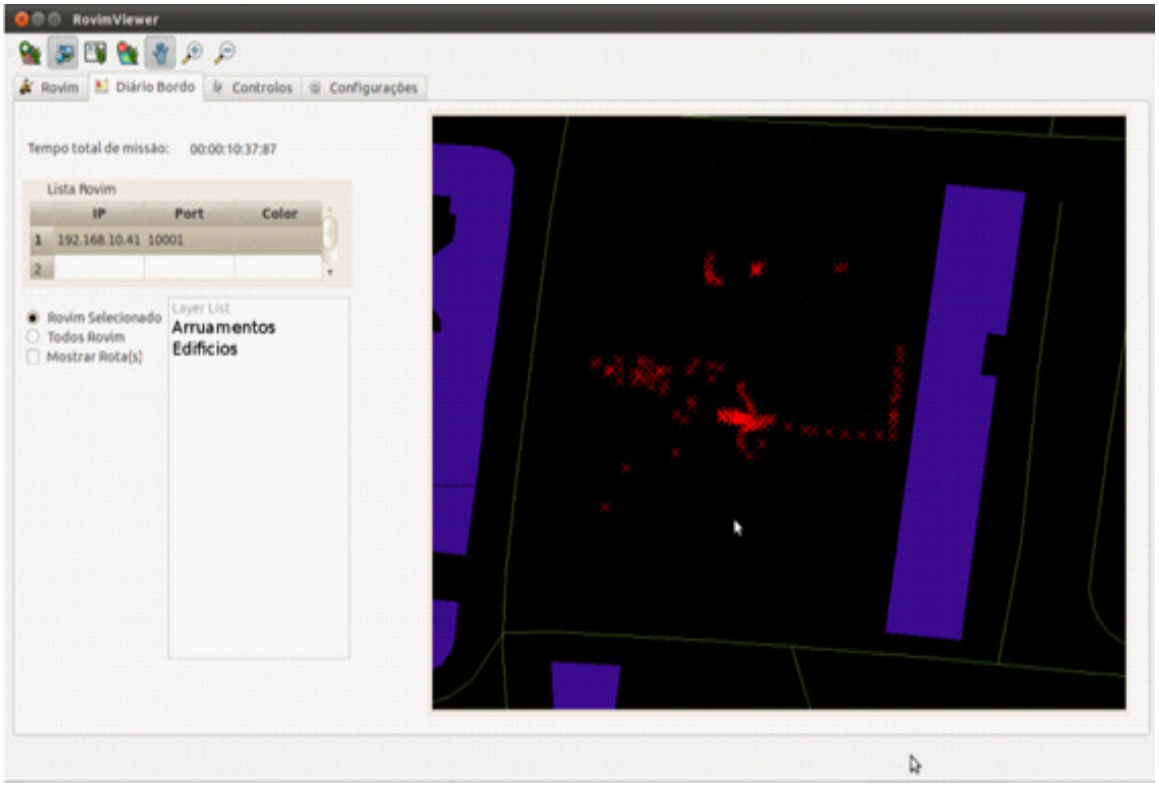


Figura 5 – Diário de Bordo.

O software desenvolvido detém outras funcionalidades como a escolha da qualidade de imagem da câmara do UxV, Figura 7, a utilização de joystick e o controlo do desvio de direcção, devido aos problemas de offset de direcção que podem provocar, aquando do deslocamento em frente do UxV, um deslize para a direita ou esquerda Figura 6



Figura 6 – Offset de deslocamento



Figura 7 – Configuração da Câmara

3. TESTES – UTILIZAÇÃO E APRENDIZAGEM

O sistema acima mencionado foi pensado de forma a permitir uma utilização simples, fácil aprendizagem e ter um controlo suave para um novo utilizador. No que diz respeito aos objetivos simplicidade e operacionalidade, pode referir-se que a aplicação foi submetida a testes conduzidos por pilotos alheios ao desenvolvimento da mesma, tendo-se concluído que os mesmos foram atingidos na sua globalidade. Os testes atrás mencionados tiveram por base um percurso desenvolvido para o efeito, com cerca de 36m, como ilustrado na figura 8. Nesse percurso, estiveram presentes o contorno de obstáculos, a utilização de dois Robôs distintos e a medição temporal de três tentativas:

1ª Tentativa – Familiarização com a aplicação – try1

2ª Tentativa – Adaptação à dinâmica do controlo – try2

3ª Tentativa – Observação de Controlo e adaptação consolidada sem prática – try3

No ensaio participaram 7 militares de ambos os sexos. O percurso inicia-se na linha vermelha, descreve o "8" em torno dos obstáculos, posiciona-se junto a uma parede onde se encontra um papel com o endereço IP do 2º robô de vigilância, momento em que se troca o controlo para esse novo IP. No controlo do 2º robô, procede-se ao deslocamento em frente até o posicionar no quadrado delimitado por 4 objetos. Após o posicionamento deste, retorna-se ao 1º robô descrevendo o restante percurso a azul.

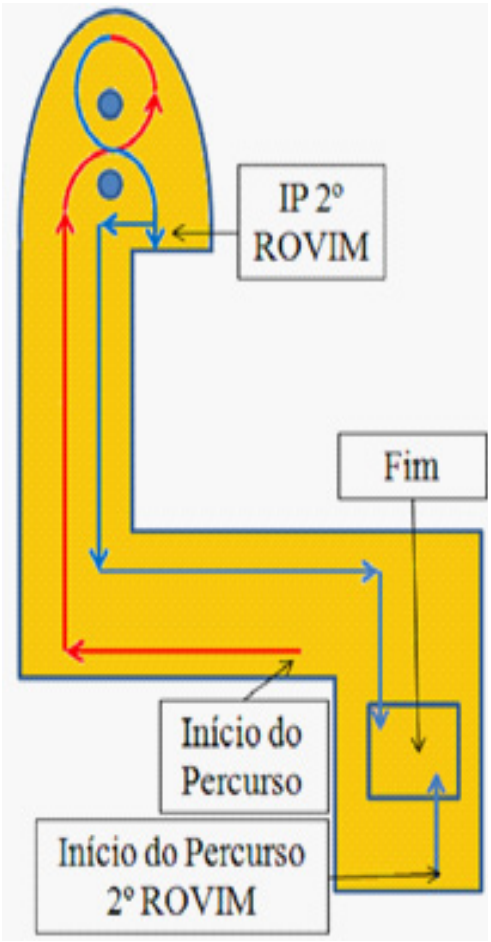


Figura 8 – Percurso de teste de adaptação.

Do teste efetuado resultou a tabela 1. Estão presentes as 3 tentativas, assim como os respetivos tempos para cada um dos sete pilotos de teste.

	PT1	PT2	PT3	PT4	PT5	PT6	PT7	Média
try1	3'22"82	3'49"82	4'30"95	3'41"28	4'52"83	3'52"98	4'30"09	04'05"82
try2	3'07"29	2'22"65	2'55"87	2'26"15	2'26"66	2'50"71	2'40"94	2'41"47
try3	2'21"47	2'06"15	2'46"37	2'00"53	2'15"78	2'25"85	2'08"37	2'17"79

Tabela 1 – Tempos de Adaptação

Face aos tempos obtidos, decidiu-se construir uma nova tabela de forma a verificar se o desvio padrão traduz uma convergência dos tempos para um determinado valor. Verifica-se então pela tabela 2 que existe uma convergência de tempos uma vez que o desvio padrão diminui para metade. Contudo, o tempo para um individuo treinado será perto de 2'. Ainda assim, pode-se observar que em 3 tentativas os tempos diminuem para cerca de metade, o que mostra que é uma aplicação simples e com o essencial para navegar no terreno.

Média	Desvio Padrão
4'05''82	32''40
2'41''47	18''80
2'17''79	15''40

Tabela 2 – Desvio Padrão

Outra possibilidade da aplicação é a construção de relatórios militares como a TUTELA ou o RELIM. Como exemplo disso, observa-se a figura 9 onde está presente um relatório TUTELA com base na imagem obtida por intermédio da aplicação e da câmara disponível no robô. Ainda que em fase de desenvolvimento, é uma possibilidade de implementação relativamente simples face a todo o projeto já desenvolvido.



Figura 9 – Relatório TUTELA Construído a partir da imagem disponível do robô.

Este sistema tem ainda o potencial de poder vir a ser utilizado em resposta a catástrofes, nomeadamente em buscas por entre os escombros. Neste contexto, apresenta-se na próxima secção os sistemas autónomos atualmente usados. Para além da resposta a catástrofes, é feita também uma abordagem a um sistema de prevenção de catástrofes.

4. IMPLEMENTAÇÃO DE SISTEMAS AUTÓNOMOS E REMOTOS NA SEGURANÇA DE POPULAÇÕES

Este tipo de sistemas (autónomos), têm sido utilizados diversas vezes e de forma eficaz em situações de calamidade. Existe em Portugal o sistema Raposa, figura 10, que permite procurar sobreviventes nos escombros.



Figura 10 – Sistema ao serviço de Portugal – Raposa

O sistema existente não é, no entanto, considerado um sistema de prevenção eficaz por não possuir antevisão de acontecimentos e respetiva divulgação dos dados em tempo oportuno. Seria oportuno dotar este tipo de sistemas de algum controlo preditivo ou de deteção instantânea. No entanto, para o conseguir, é fundamental dotar também os processos no terreno de monitorização específica (sensores) em que a recolha de dados possa ser partilhada, preferencialmente em rede, de modo a dotar os decisores de informação qualitativa e quantitativa em tempo útil permitindo uma tomada de decisão mais assertiva.
Terramotos, acidentes industriais, inundações e tempestades, são eventos que provocam mais danos físicos e humanos em torno das populações. O Instituto Português de Meteorologia possui instrumentação capaz de permitir detetar em tempo real determinado acontecimento. Deste modo seria possível a utilização de sistemas autónomos que funcionem em comunicação permanente com uma rede que possa disponibilizar serviços para as comunicações GSM e rede de dados nacional/internacional. Este sistema permitiria,

por exemplo, no caso de um tremor de terra na região de Lisboa, emitir um alerta dirigido à população em geral como medida preventiva para possíveis inundações. Sendo possível que o período de tempo ganho entre o alerta e o acontecimento possa servir para acionar, por exemplo, planos de evacuação e mobilização de meios por parte das autoridades competentes.

Este sistema funcionaria assente em cima de câmaras fixas de vigilância, remotamente controladas, e com um sistema de localização. Distribuir-se-ia informação via GSM, redes sociais, mail, mensagens instantâneas – sms, para os indivíduos que se encontrassem ligados na célula de comunicações na área afetada. Isto iria permitir evacuar as pessoas de um modo mais rápido, pois seriam alertadas instantaneamente. Contudo, as forças que apoiam em resposta a este tipo de situações, também elas poderiam começar a mobilizar meios para atuar. Não só se iria alertar a população, como também se iriam informar as forças que iriam responder à calamidade (Proteção Civil, Exército, Força Aérea, Marinha, GNR, PSP, Bombeiros,…) que de um modo mais rápido chegariam ao estado de prontidão de resposta à calamidade.

O objetivo é informar de forma rápida e autónoma através de redes sociais, moveis ou de banda larga, para situações como:

- Terramotos;
- Tsunami;
- Incêndios;
- Acidentes industriais;
- Ondas de calor/frio;
- Colapsos estruturais;
- Explosões;
- Acidentes Rodoviários;
- Naufrágios;
- Quedas de pontes.

Todas as situações consideradas de calamidade têm a possibilidade de serem identificadas por sistemas sensoriais ou de vigilância remota que permitam disseminação de informação via rede de dados. É apresentado então um esquema concetual de interação do sistema de informação para a segurança na figura 11.

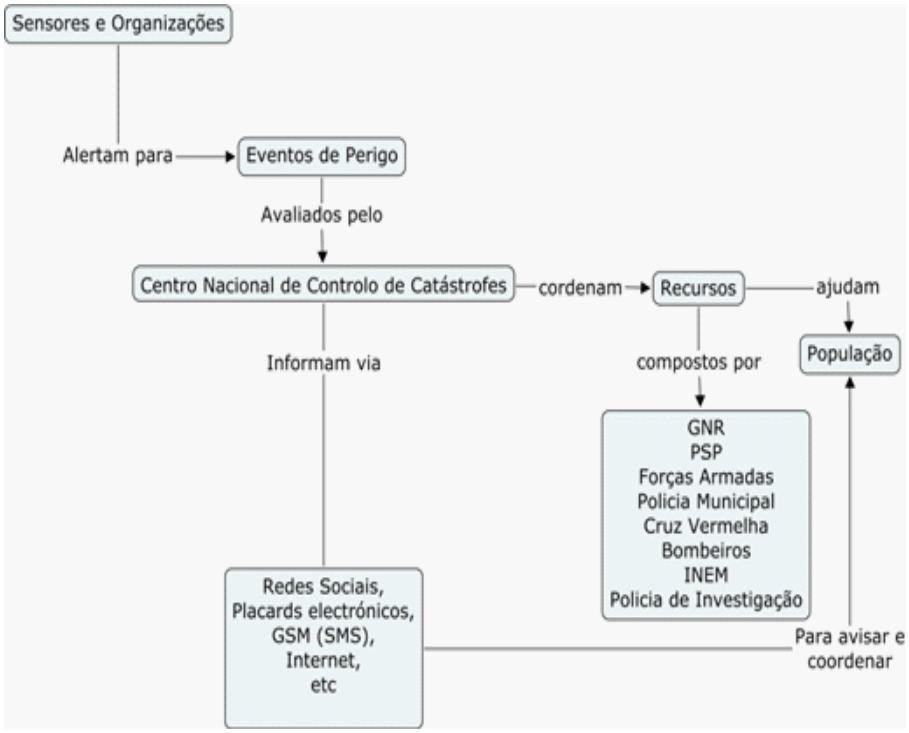


Figura 11 – Mapa Conceptual para o Sistema de Informação.

Após serem dados os alertas e já estar a decorrer o incidente, entrariam no modo de busca e salvamento os sistemas remotamente controlados. Neste caso, as reduzidas dimensões dos dispositivos de procura remota são essenciais de modo a facilitar a abordagem aos diversos obstáculos, bem como permitir a sua entrada nos escombros existentes. Esses UxVs podem ser terrestres como o "Raposa" ou o "Rovim" ou podem ser baseados em quadrotores como o observado na figura 12.

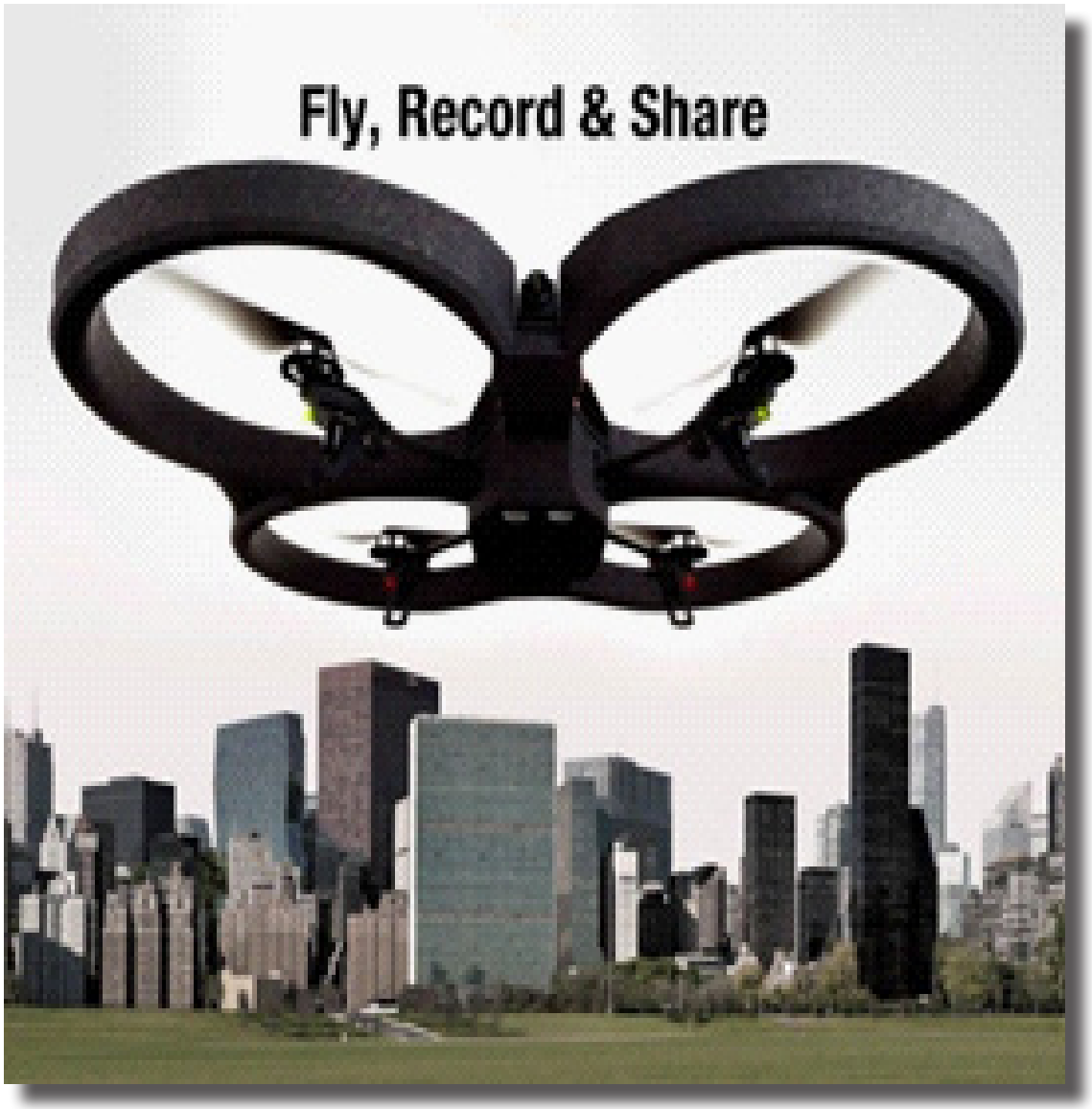


Figura 12 – Ar. Drone Parrot [2]



5. CONCLUSÃO

Facilmente se percebe a necessidade de existência dos sistemas autónomos de vigilância e reconhecimento, pois uma vez em tempo de paz, podem ser usados para coordenar, reconhecer e auxiliar equipas nas operações de busca e salvamento. Em caso de conflito, deixa de existir a necessidade de utilização primária de meios humanos em terreno hostil nas operações de reconhecimento. Desse modo, também pode existir um aproveitamento dos recursos das forças armadas para melhor servir Portugal e a população. Neste artigo está presente um exemplo da capacidade do exército em desenvolver ou colaborar no desenvolvimento de equipamentos capazes de prestar serviço fora das fronteiras de ação primária do exército, apresentando-se o desenvolvimento de um sistema autónomo de vigilância.

Referências

[1] Tiago Argentino Matos Santos. Rovim - robot de vigilância de Instalações militares – comunicações e posto de controlo. Dissertação de Mestrado, AM - Academia Militar e IST-Instituto Superior Técnico, Outubro 2011.
[2] Parrot AR.Drone 2.0, http://news.softpedia.com/newsImage/CES-2012-iPhone-Controlled-Quadricopter-AR-Drone-2-0-Gets-New-Design-HD-Cam-2.jpg/, consultado em, 11/02/2012

Bibliografia

Jorge Manuel Estrela da Silva. Software para controlo e gestão de missões de veículos autónomos. Dissertação de Mestrado, FEUP-Faculdade de Engenharia do Porto, 2001.
Serviço Nacional de Proteção Civil, http://www.snpc.cv, consultado em, 23/10/2010
Proteção civil, http://www.proteccaocivil.pt/, consultado em, 23/10/2010
Ministério da administração interna, http://www.mai.gov.pt/, consultado em, 23/10/2010
Eduardo Alexandre Pereira da Silva. Controlo de veículos autónomos. Tese de Doutoramento, FEUP-Faculdade de Engenharia do Porto, 2002.

Projecto, Realização e Estudo de um Agregado de Fendas

1. INTRODUÇÃO



ALF TPO JOÃO MONTEIRO

Actualmente, a comunicação sem fios permite estabelecer a comunicação entre dois dispositivos, mediante a propagação de ondas eletromagnéticas (p.e. ondas de rádio, luz infravermelha, laser, etc). Na indústria de telecomunicações, a sua aplicabilidade é notável nos transmissores e receptores de rádio, controlos remotos, redes de computadores, entre outros. Neste âmbito, as antenas constituídas por fendas assumem maior relevância no sistema de comunicação sem fios (Wireless). Uma fenda num guia de ondas metálico é um elemento radiante. O seu comportamento é idêntico ao funcionamento de um dípolo elétrico. Por analogia, um agregado de fendas apresenta comportamento idêntico ao de um agregado de dipolos. É neste contexto que surge o objectivo primário desta dissertação: a análise de uma antena constituída por guia de ondas.

A antena é constituída por um guia de ondas rectangular, com 4 fendas realizadas no plano zy. Neste capítulo é possível compreender o seu modo de funcionamento.

Guia de ondas

O Guias de onda usado como elemento base destas antenas foi fabricado a partir de um perfil de alumínio anodizado, o que se traduz num baixo custo para estas antenas e também na facilidade do seu fabrico, duas características importantes sobretudo em aplicações militares. Estes guias foram dimensionados de modo a operarem no modo fundamental TE10.

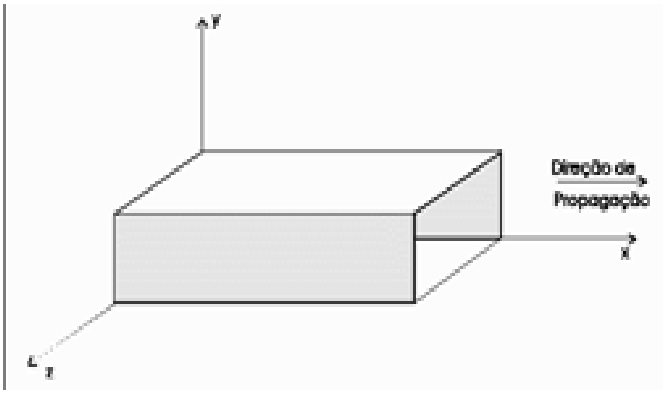


Figura 1 – Guia de ondas Rectangular

As medidas dos guias utilizados podem ser observados na tabela 1.

Tabela 1 – Dimensões do guia de ondas

	Dimensões (mm)
Largura (a)	37
Comprimento (b)	97
Espessura	1,5

Modo fundamental

O Modo Fundamental de propagação, nos guias com as dimensões referidas anteriormente, é o modo TE10. Este modo tem como frequência de corte 1,55GHz, o que permite portanto a operação na frequência central de trabalho, 2,45GHz.

Tipo e Posicionamento das fendas

Um dipolo de meia onda ressonante ou uma fenda ressonante tem um comprimento de $0{,}475\lambda_0$ (1). Elliott e Kurtz concluíram que o comprimento da fenda vem dado por $0{,}483\lambda_0$. (2)

Os mesmo autores, com recurso às curvas de Stegen, determinaram que a largura da fenda é dada por:

$$W = (1.5875a)/(22.86) \quad [mm]$$

No entanto, para a antena em estudo foram realizadas simulações de forma a optimizar a largura da fenda. Na tabela seguinte é possível visualizar as medidas das fendas

Tabela 2 – Características da fenda

Antena	Plano ZY
L (comprimento) (mm)	59
W (largura) (mm	7

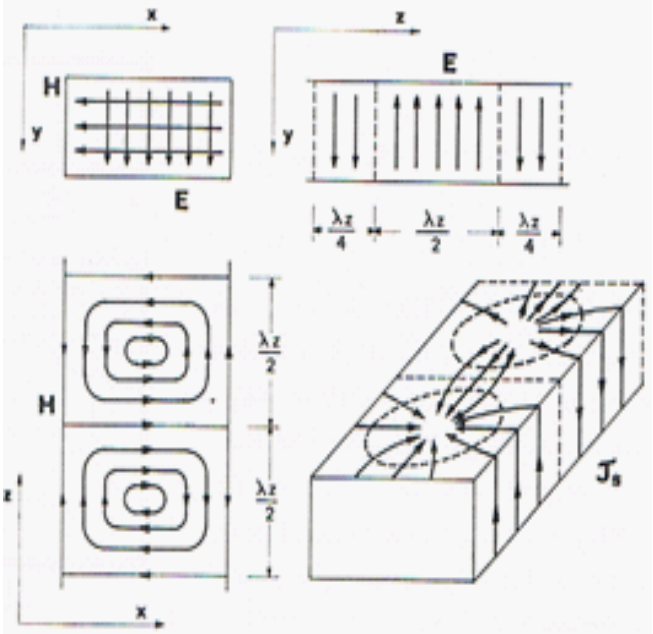


Figura 2 – Distribuição das linhas de campo magnético, eléctrico e corrente superficial (3)

Com base nesta estrutura de linhas de corrente (Figura 2) dimensionou-se as fendas para que tivessem um máximo de radiação. As linhas de corrente têm uma distribuição ao longo do guia de acordo com a figura 2. Esta distribuição pode ser expressa pelas seguintes expressões:

$$\mathbf{J} = \mathbf{n_p} \times \mathbf{H}$$

$$J_y = -e_x \times H_z e_z$$

$$H_z = H_{z_0} \cos(\frac{\pi}{a} x)\ \cos(\omega t - k_z z)$$

Estas expressões, bem como a distribuição das linhas de corrente da Figura 2, são essenciais para perceber o posicionamento das fendas na antena com fendas no plano zy. As fendas encontram-se colocadas no plano zy correspondentes aos pontos de convergência e de divergência das linhas de corrente elétrica (plano zx). A disposição das fendas ao longo do guia pode ser observada na Figura 3.



Figura 3 – Antena

2. SIMULAÇÕES E MEDIDAS EXPERIMENTAIS

Inicialmente utilizou-se, nas simulações, uma antena desadaptada. Os resultados obtidos estão presentes na Tabela 3.

	3D	Plano H	Plano E
S11 (dB)		-6,26	
VSWR		2.9	
Ganho (dBi)	10,01	10,0	10,0
NLS (dB)	-	4,25	6,28
Largura de feixe a -3dB	-	10,3º	147,7º

Tabela 3 – Simulação da antena sem stub

Como é possível visualizar na tabela, os valores de S11 (-6,26dB) e do VSWR (2,9) espelham a desadaptação da antena.
Posteriormente a antena foi adaptada com recurso a um stub, dimensionado primeiramente recorrendo à Carta de Smith e posteriormente otimizado por simulações sucessivas. Para esta antena o stub encontra-se a 40mm do topo do guia e tem uma profundidade de 13mm.
Procedeu-se então à análise dos resultados obtidos por simulação da antena já adaptada.

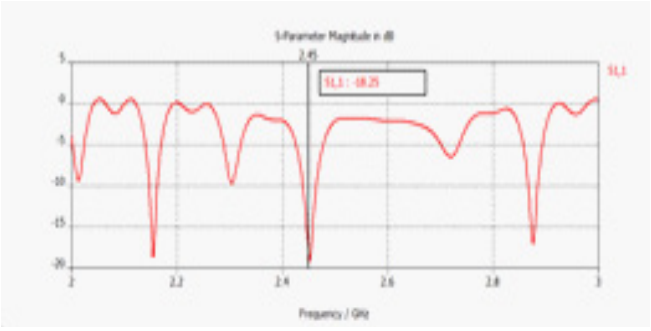


Figura 4 – S11 (Simulação)

Através da análise da figura 4 verifica-se que a antena apresenta um valor de S11 de -18,25dB, o que se traduz num VSWR de 1,279. Estes valores permitem afirmar que a antena se encontra adaptada.

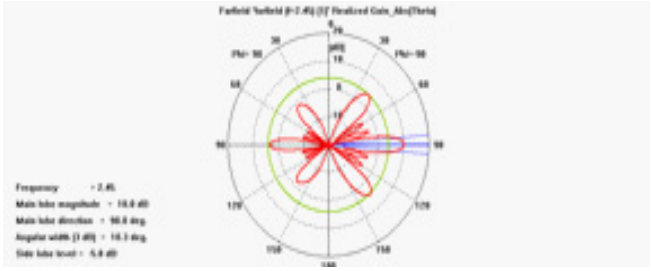


Figura 5 – Diagrama de Radiação (Plano H)

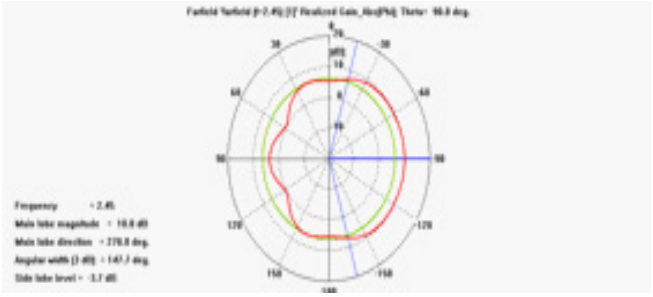


Figura 6 – Diagrama de Radiação (Plano E)

Analisando a figura 5, é possível observar que para o plano H a antena possui um lóbulo principal com aproximadamente 11dB de ganho e um nível de lóbulos secundários (NLS) de -3,7dB. Do mesmo modo é possível analisar a figura 6, onde o ganho tem um valor de 10dB e um NLS de -3,7.

Medidas experimentais

Figura 7 – S11 (Experimental)

No gráfico 7 é possível observar que o S11 experimental tem um valor muito próximo de -15dB. Este valor encontra-se muito próximo do valor mínimo aceitável que é -15dB. Apesar de estar de estar ligeiramente acima do valor pretendido considera-se aceitável.

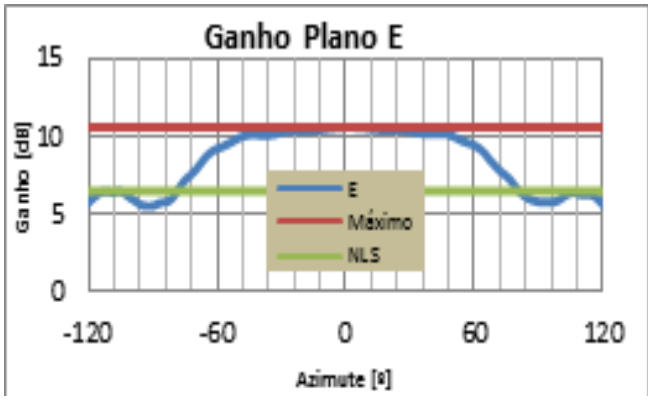


Figura 8 – Ganho (Plano E)

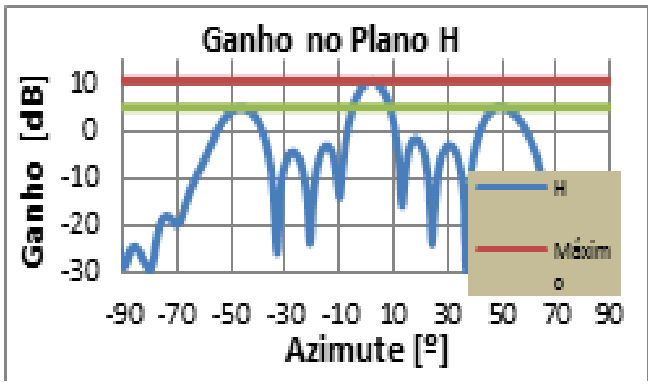


Figura 9 – Ganho (Plano H)

Nas figuras 8 e 9, a azul tem-se a distribuição do ganho ao longo do azimute, a vermelho o valor máximo atingido e a verde o nível de lóbulos secundários. É de salientar a elevada amplitude dos lóbulos secundários, o que pode causar interferência na radiação. O resumo dos resultados obtidos nos dois gráficos anteriores bem como as restantes medidas experimentais está presente na Tabela 4.

Tabela 4 – Medidas experimentais

	Plano H	Plano E
S11 (dB)	-13,8	
VSWR	1.52	
Ganho Realizável (dBi)	10,75	10,61
NLS (dB)	5,18	6,48
Largura de Feixe (-3dB)	9	146

3. COMPARAÇÃO ENTRE SIMULAÇÕES E RESULTADOS EXPERIMENTAIS

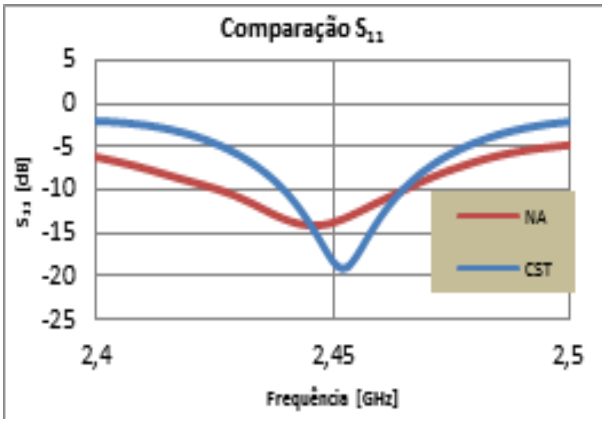


Figura 10 – Comparação S11

Os valores de S11, experimental e simulado (experimental a vermelho e simulado a azul), não têm o mesmo valor, apresentando uma diferença aproximadamente de 3dB. Este facto pode dever-se ao ajuste manual do stub, e à dificuldade em colocar o mesmo a uma profundidade exacta de penetração no guia.

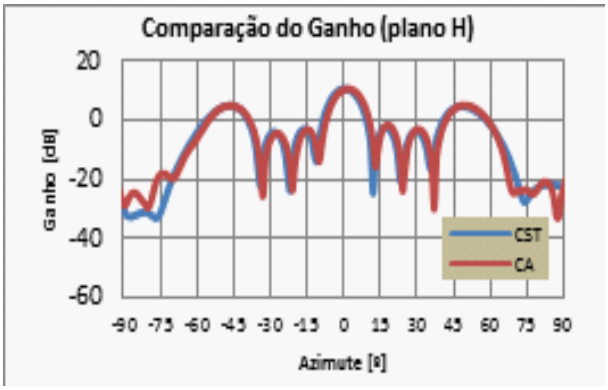


Figura 11 – Comparação (Ganho plano H)

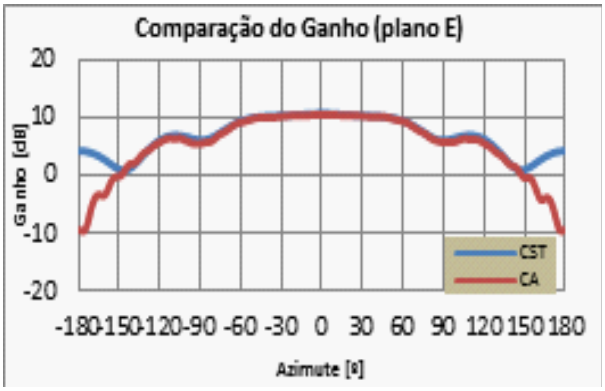


Figura 12 – Comparação (Ganho plano E)

As figuras anteriores demonstram que a distribuição do ganho, no plano H ou no plano E, coincidem quase sempre ao longo de todo o gráfico. Pode concluir-se que antena, para estes dois parâmetros, apresenta-se como uma antena ideal. Para uma melhor percepção da comparação entre resultados experimentais e simulações apresenta-se a Tabela 5.

Tabela 5 – Comparações (Resumo)

	Resultados obtidos por simulação		Resultados obtidos experimentalmente	
	Plano H	Plano E	Plano H	Plano E
S11(dB)	-18.25		-13,8	
VSWR	1,28		1,52	
Ganho Realizável (dBi)	10,8	10,8	10,75	10,61
NLS (dB)	5,1	7,1	5,18	6,48
Largura de Feixe (-3dB)	10,3	147,9	9	146

4. CONCLUSÕES

A elaboração deste trabalho, teve como objectivo inicial, o dimensionamento, a construção e a análise de uma antena constituída por um guia de ondas. Dividiu-se a análise em duas partes, medidas obtidas por simulação e medidas obtidas experimentalmente. Finalmente compararam se as medidas obtidas nas duas situações de forma a validar resultados.
Seguidamente, é possível observar os diagramas de radiação 3D da antena em estudo.

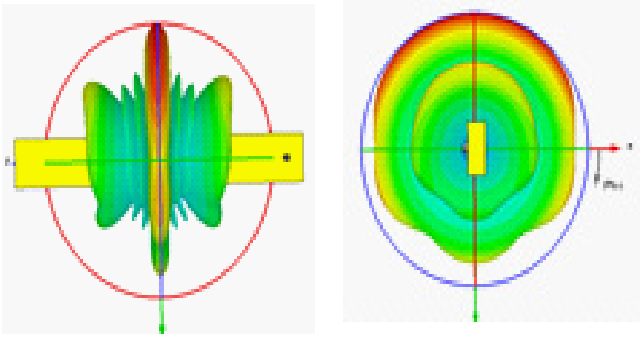


Figura 13 - Diagramas de Radiação 3D

Pela observação dos gráficos anteriores pode concluir-se quanto às principais características da antena em estudo, isto é, a antena é praticamente isotrópica no plano E e é muito diretiva no Plano H.

REFERENCES

1. Kraus, John D. Antennas. s.l. : McGraw-Hill Book Company, 1950.
2. Wade, Paul. Microwave Antenna Book. 2003.
3. Faro, M. de Abreu. Propagação e Radiação de ondas Electromagnéticas. s.l. : Técnica AIST, 1984.

Estudo das perturbações dos geradores eólicos na radiação das estações de suporte à navegação aérea



ALF TPO HUMBERTO COSTA

1. Introdução

Hoje em dia, a navegação aérea é baseada em sistemas electrónicos de rádio frequência. Os sinais desses sistemas podem sofrer interferências que alterem as suas rotas e/ou as suas potências, tais como atenuações, reforços ou distorções. Essas interferências são causadas por obstáculos na direcção de propagação dos sinais ou simplesmente por reflexões no terreno circundante a estes sistemas. Assim, e visto que, a crescente procura, do Homem, por uma fonte de energia limpa, viável e rentável, para substituir aquelas baseadas em combustíveis fosseis, levou-o a criar grandes parques eólicos por todo o mundo, estes tornaram-se um potencial elemento causador de interferências nos sinais de auxilio à navegação aérea.

2. Caracterização das fontes dos sinais

Foram estudados dois sistemas de rádio - ajudas à navegação aérea, o VOR ("Very High Frequency Omnidirection Range") e o RADAR ("Radio Detection And Ranging").
O sistema VOR consiste num grupo de emissores, geograficamente distribuídos e um receptor a bordo de uma aeronave. As estações de solo são compostas por um aglomerado circular de antenas como uma das antenas no centro. A antena central é omnidireccional e a sua radiação é de fase fixa, enquanto as outras são direccionais e a sua radiação é de fase variável. Tipicamente, uma estação de solo apresenta um ganho de 5dBi e os receptores apresentam um ganho de 5 ou 2,15dBi, dependendo do tipo de aeronave. A potência emitida por uma estação de solo é de aproximadamente 50W com uma polarização horizontal, na banda dos 108MHz aos 118MHz, apresentando uma sensibilidade de recepção de -129dB. O sistema VOR emite dois sinais diferentes, simultaneamente. Um sinal omnidireccional e de fase fixa através da antena central, este sinal indica a direcção do Norte Magnético. O outro sinal é transmitido pelas antenas circundantes, aos pares diametralmente opostos. A bordo, é calculada a diferença de fase entre os dois sinais recebidos e converte essa a diferença em graus magnéticos.



Figure 1 - Estação de solo VOR

O sistema de Radar é um equipamento que detecta e localiza alvos através de ondas rádio de UHF. Este sistema é dividido em dois tipos: o PSR ("Principal Surveillance Radar") e o SSR ("Secundary Surveillance Radar"). Estes dois sistemas podem estar co-localizados na mesma estrutura física.



Figure 2 - Sistema de Radar PSR e SSR na mesma estrutura física

A missão do PSR é localizar a aeronave, operando nos 2700-2900MHz com 34dBi de ganho e uma polarização linear ou circular dependendo das condições climatéricas, apresenta uma sensibilidade de -104dB e uma potência de emissão de 15kW. Este sistema não necessita de nenhum dispositivo a bordo da aeronave porque capta os seus próprios ecos reflectidos pelos seus alvos.

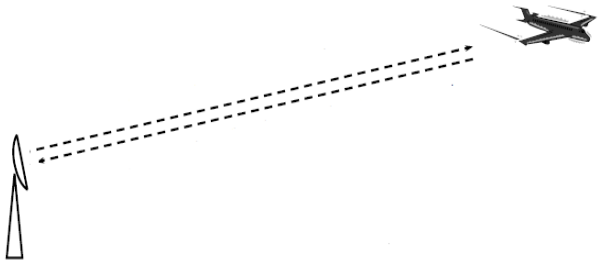


Figure 3 - Modo de operação do PSR

A missão do SSR é identificar a aeronave. Este sistema necessita de uma transmissões/receptor a bordo da aeronave (transponder). A estação de solo emite um sinal de 1,6kW com um ganho de 27dBi. Os transponders operam na banda dos 1030-1090MHz com uma potência de emissão de 250w e uma sensibilidade de -90dBm, apresentam um ganho de emissão de 7,5dBi e um ganho de recepção de 5,9dBi. Este sistema é capaz de medir a altitude, a distância e o azimute da aeronave. O seu funcionamento consiste no envio de interrogações codificadas (up-link) às quais os transponders respondem coma sua identidade, a sua altitude e azimute (down-link) nos 1090MHz.

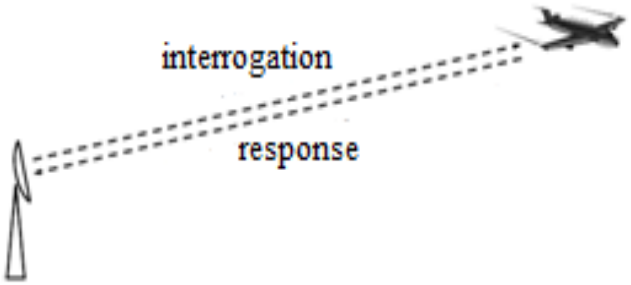


Figure 4 - Modo de operação do SSR

3. Fontes de interferência e seus efeitos

As fontes de interferência aqui estudadas são os geradores eólicos tipo hélice, de eixo horizontal com três pás (de 40m cada) e um mastro de 80m e apresentam uma potência instalada de 2MW. São os geradores mais comuns numa estação eólica.

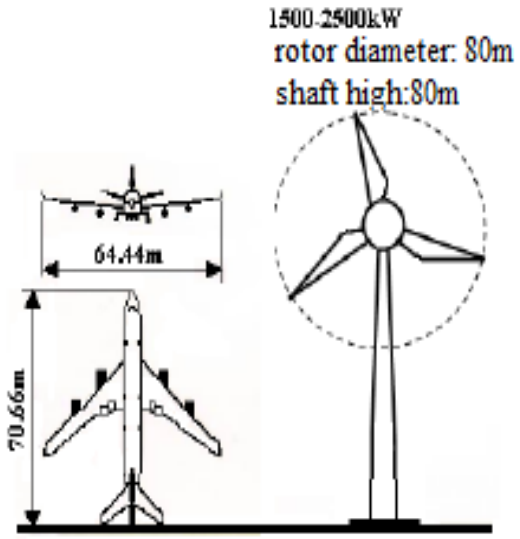


Figure 5 - Comparação entre um gerador eólico e um Boeing 747, uma aeronave usada na aviação civil

Este tipo de obstáculos não aparece isolado no espaço, mas sim em grupos que são chamados de estações eólicas. Estes obstáculos apresentam vários factores que têm influência nas perturbações sobre sinais de rádio-frequência. Exemplos desses fatores são: os geográficos, os físicos e as características rádio elétricas. Quando uma onda electromagnética atinge uma estação eólica, as interferências causadas são mais severas do que se esta atingisse apenas um gerador. Assim este tipo de obstáculo pode causar, no limite a perda total do sinal à sua retaguarda.
A presença de estações eólicas perto dos de dispositivos de rádio-ajuda à navegação aérea pode introduzir vários efeitos que afectam a performance dos sinais dessas rádio-ajudas. Esses efeitos são:

- Efeitos de campo próximo;
- Difracção;
- Reflexão e/ou scattering;
- Efeito sombra;

3.1. Efeito de campo próximo

Na zona próxima de uma antena é demasiado difícil prever o comportamento dos campos indutivos e efeitos causados por obstáculos que ai existam. Essa zona aumenta com o aumento do diâmetro da antena e da frequência de operação.

3.2. Difracção

Qualquer obstáculo pode modificar a amplitude e fase de uma onda electromagnética, e este efeito não é limitado apenas aos materiais bons condutoras, mas também abrange os materiais bons dieléctricos. Este efeito pode ser evitado se se garantir que qualquer obstáculo está fora dos limites de uma zona particular, chamada de Zona de Exclusão de Fresnel.

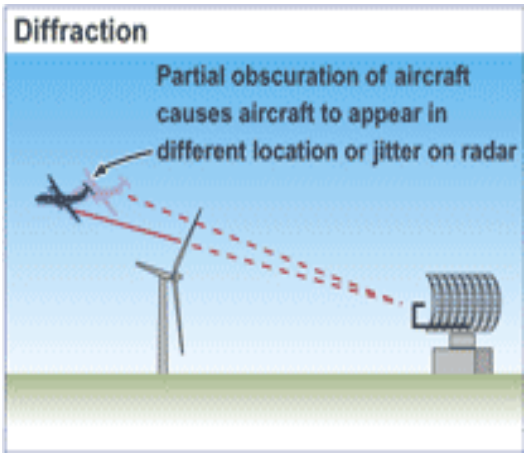


Figure 6 - Efeito de Difracção de uma sinal de radar num gerador eólico (Flightglobal, 2006)

3.3. Efeito de reflexão e/ou scattering

Este efeito ocorre quando um objecto interfere com uma frente de onda e reflecte e/ou espalha o sinal. Este efeito causa a degradação do sinal se um dos sinais reflectidos atingir o receptor. Em suma é necessário estabelecer uma zona de exclusão para evitar este efeito.

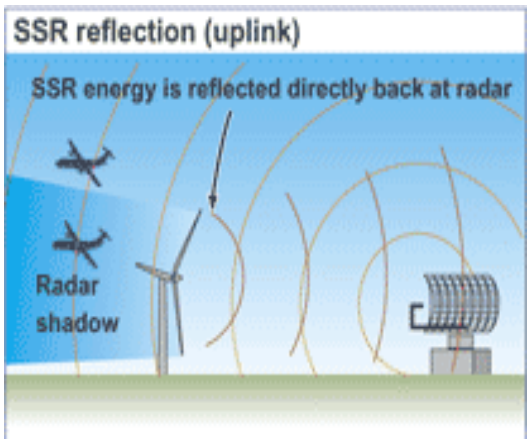


Figure 7 - Reflexão de um sinal de radar por um gerador eólico (Flightglobal, 2006)

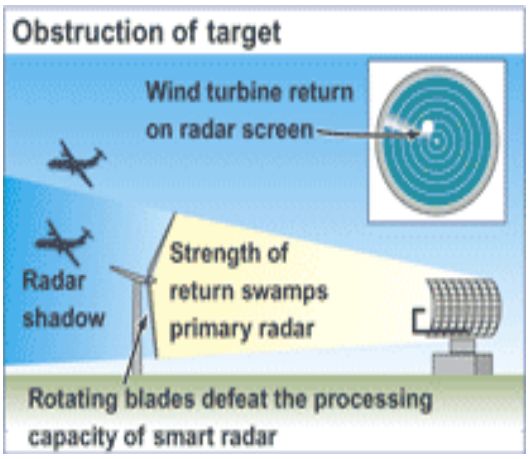


Figure 9 -Obstrução e efeito de sombra criado por um gerador eólico

Foram estudados três diferentes tipos de reflexão, reflexão apenas nas pás dos geradores, reflexão apenas no terreno envolvente e reflexão no terreno envolvente e nas pás do gerador:

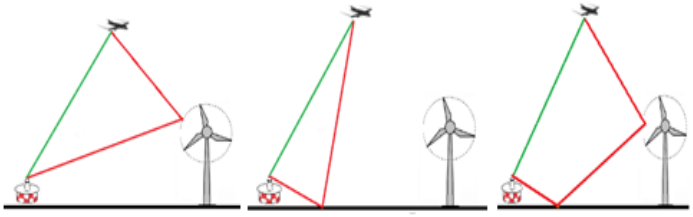


Figure 8 - modelos usados no estudo do efeito de reflexão

3.4. Efeito sombra

Este é o clássico efeito introduzido pela presença de um obstáculo na direcção de propagação de uma onda. Esses obstáculos podem causar a perda total do sinal à sua retaguarda. O tamanho dessa sombra aumenta se se pensar em grandes estações eólicas.

4. Conclusão

Na seguinte tabela são mostradas as zonas de exclusão para os diferentes efeitos:

Tabela 1 -Zonas de Exclusão para os diferentes sistemas estudados

	System	FIZ	ERZ	ENFZ
Distance [Km]	VOR/ DME	1440	5	42,55
	PSR	200	-	121,7
	SSR uplink	320	-	124,3
	SSR downlink	-	-	-

Para o sistema VOR estas distâncias não são fáceis de manter porque este tipo de sistema está, geralmente, instalado em terreno alto da mesma forma que as estações eólicas. Para os sistemas de radar, estas distâncias são fáceis de manter porque, geralmente, estão localizados dentro dos perímetros de aeroportos ou aeródromos que estão desimpedidos deste tipo de obstáculos. Nas ligações de downlink no sistema de radar SSR não existem distâncias de segurança porque, em princípio, não existem obstáculos nas imediações de uma aeronave em pleno voo.

Bibliografia

Faculdade de Engenharia da Universidade do Porto. Sistemas de localização aérea via rádio . Sistemas de localização aérea via rádio . [Online] 2002-2003. http://paginas.fe.up.pt/~hmiranda/st2/radio_ajudas_relatorio.pdf.

NRPL Group. PSR MORAVA M10. RADAR TECHNOLOGIES. [Online] 2002-2011. http://www.nrplgroup.com/products/psr_morava_m10/.

Oswaldo Massambani, Ph.D. Princípios do RADAR. São Paulo : Universidade de São Paulo, 2007.

Forecast International. SSR/MSSR ATC Radar Series (Raytheon). Canada : s.n., 2001.

Agence Nationale des Fréquences. Guide sur la problema de la perturbation du fonctionnement des radars par les eoliennes. Commission Consultative de la Compatibilité Electromagnétique. França : s.n., 2007.

Bacon, D F. Fixed-links wind-turbine exclusion zone method. 2002. p. 143.

EUROCONTROL Guidelines. EUROCONTRL Guidelines on How to Assess the Potential Impact of Wind Tubines on Surveillance Sensors, 2010.

Professora Doutora Maria João M. Martins. Propagação e Radiação de Ondas Electromagnéticas, Radiação, 2002.

Professora Doutora Maria João M. Martins. Propagação e Radiação de Ondas Electromagnéticas, Conceitos Fundamentais, 2002.

Signal Captains Career Course



Cap Tm (Eng.) Pedro Grifo

No dia 08 de Março de 2011 iniciou-se o quarto curso Signal Captains Career Course (SCCC 04-11) de 2011, em U.S. Army Signal Center and Fort Gordon (Augusta, Geórgia) nos Estados Unidos da América com a duração de 20 semanas. Este curso contou com a presença de 4 alunos internacionais e 34 alunos americanos. A Companhia Charlie, do Batalhão de Transmissões Nº442, tem a responsabilidade de organização do SCCC.

Antes de se iniciar o SCCC, realizou-se um curso de curta duração designado de Prep-International Course, unicamente para alunos internacionais, com o intuito de transmitir conhecimentos acerca da rotina da unidade, promover relações interpessoais e facilitar a adaptação ao sistema de ensino militar americano. Neste curso as aulas desenrolaram-se sob a forma de debate/discussão, onde se abordaram diversos assuntos de caráter geral acerca dos Estados Unidos da América. As temáticas abordaram assuntos desde a economia, passando pelo seu sistema judicial, sistema político, História e o chamado American way of life. Ainda durante esta fase, os alunos tiveram que preparar a sua autobiografia e um country brief que foi apresentado em público. Findas estas cerca de duas semanas, houve uma cerimónia de entrega de diplomas que contou com a presença do chefe do International Military Students Office, dos formadores e pessoal administrativo.

Finalizada esta primeira etapa, iniciou-se o SCCC 04-11 juntamente com os alunos americanos. Para melhor controlo da turma, esta foi dividida em dois grupos, cada um deles com um indivíduo equivalente a diretor de curso designado de Small Group Leader (SGL).

O SCCC tem como principais objetivos:

1. Preparar para o desempenho de funções de Comandante de Companhia e elemento de Estado-Maior de um Batalhão ou Brigada;

2. Manter/melhorar a aptidão física;

3. Desenvolver/melhorar os fundamentos de liderança;

4. Cooperar e interagir com os outros;

5. Partilha de experiências pessoais;

6. Descompressão da atividade operacional.

O curso encontra-se atualmente organizado em 4 módulos nucleares. O módulo A contempla matérias de caráter geral tais como liderança, estudo de das influências culturais, doutrina e operações todo espetro. O módulo B aborda as matérias relacionadas com o desempenho de funções como Oficial de Transmissões (S6) tais como planeamento do apoio de comunicações (Processo de Decisão Militar), Sistemas de Comando e Controlo, distribuição de energia, Information Assurance e outras. No módulo C abordam-se matérias relacionadas com o desempenho de funções como Comandante de Companhia tais como Gestão do Treino, Disciplina Militar, Manutenção, Sistemas de Transmissão e Planeamento de Comunicações. O módulo D destina-se à execução dos exercícios de armas combinadas (CAX) e de planeamento do apoio de Comunicações e Sistemas de Informação. O dia a dia inicia-se bastante cedo sendo bastante preenchido. Pelas 06h00 tinha lugar o início dos trabalhos com treino físico até às 07h00.

Na turma havia um oficial que desempenhava as funções de oficial de treino físico e tinha a responsabilidade de elaborar o horário mensal de treino físico e propor o mesmo ao SGL. As sessões de treino físico cobriam diversas atividades com treino variado, assim como corrida, treino em circuito, natação, desportos coletivos e outras.

De seguida, após um banho reconfortante e a 1ª refeição tomada dava-se o início das aulas às 08h30. Por volta das 11h30 fazia-se um alto para a 2ª refeição, retomando-se novamente as aulas às 13h00, podendo os trabalhos estender-se até às 18h00.

As aulas mais técnicas, estas eram ministradas por especialistas na área, enquanto que áreas de matérias mais gerais o formador, embora também um entendido na matéria, era ao mesmo tempo um facilitador, de forma a que os alunos, fruto das suas experiências em teatros de operações, pudessem partilhar o seu conhecimento sobre a matérias.

Algumas das matérias tratadas durante o curso eram disponibilizadas on-line na plataforma Blackboard, tendo cada aluno as credenciais para aceder aos conteúdos.

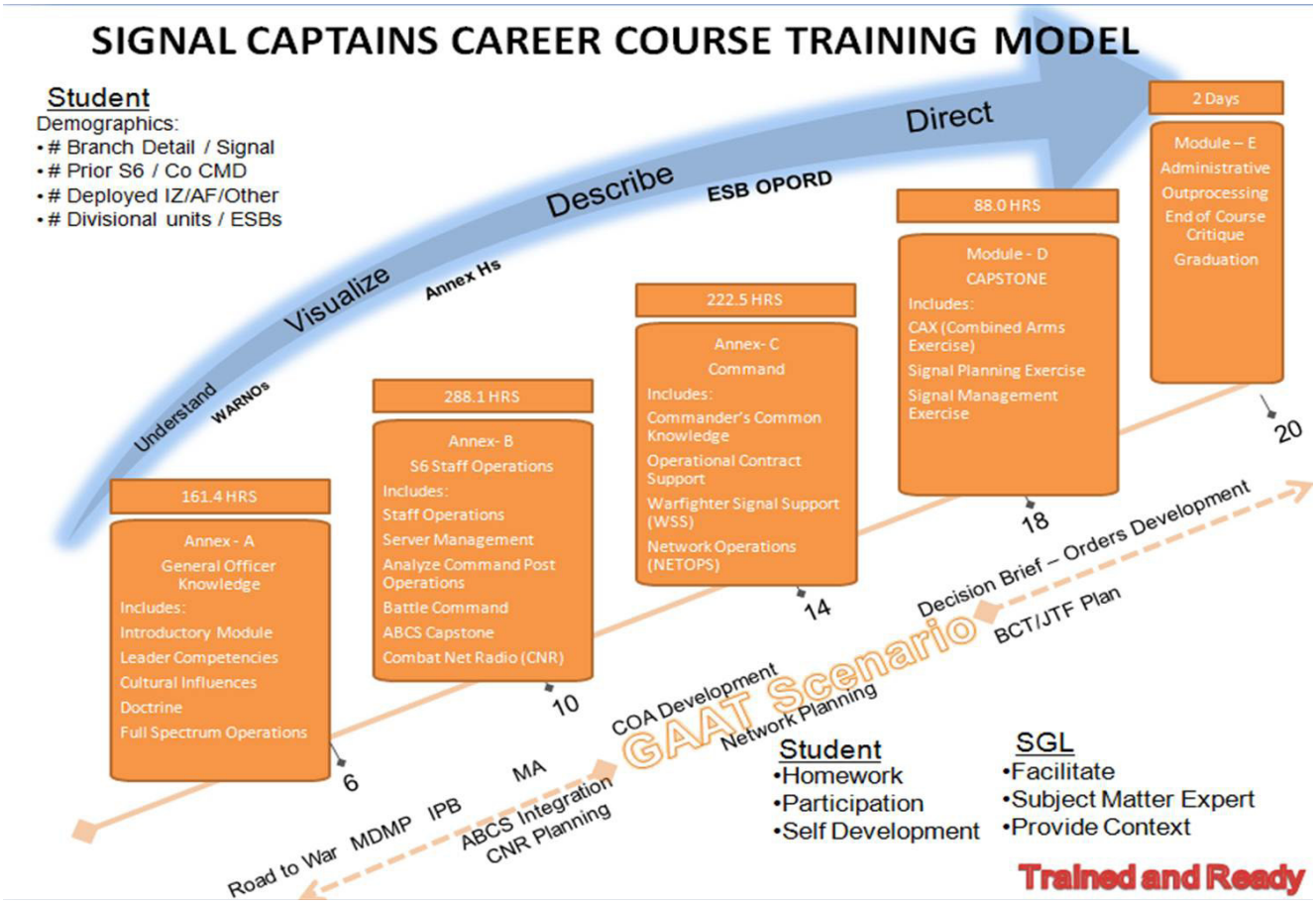


Figura 1 - Planificação do SCCC

Como actividade extra-curricular houve a possibilidade de obtenção do German Armed Forces Badge For Military Proficiency[1] , que consiste na realização de diversas provas desportivas (natação 200 m, corrida 100 m em velocidade, corrida 3 Km, salto em altura, lançamento do peso, marcha com 15 Kg de carga, tiro a 25m com pistola de 9mm) e um teste de primeiros socorros. Este distintivo é atribuído pelas Forças Armadas alemãs, tendo sido o controlo das provas efectuado pela equipa de ligação alemã que se encontra em Fort Gordon. Existem três níveis que podem ser atribuídos, designadamente bronze, prata e ouro. Os alunos internacionais aliados também têm a possibilidade de prestar provas para obtenção desta distinção e envergar o respectivo distintivo no uniforme.



Figura 2 - Entrega do Diploma e Distintivo do German Armed Forces Badge For Military Proficiency

1 http://en.wikipedia.org/wiki/German_Armed_Forces_Badge_for_Military_Proficiency

Na Unidade havia sempre diversos eventos disportivos durante o ano, entre os quais corridas de Batalhão, Brigada e de Unidade. Um dos maiores eventos desportivos realizados com participação também de atletas civis foi a prova Signal Regimental Run 10Km.



Figura 3 - Signal Regimental run 10 Km

O International Students Military Office, gabinete que tem a responsabilidade de prestar apoio administrativo a todos os alunos internacionais, organizou diversos eventos culturais de forma propiciar um melhor conhecimento da cultura americana. Para o efeito realizaram-se durante o curso três viagens a estados diferentes, sendo a primeira a Huntsville, no estado do Alabama onde se visitou o US Space and Rocket Center[1] , a segunda a Gatlinburg no estado do Tennesse onde se teve a possibilidade de assistir a espetáculos e visitar as Smooky mountains e a terceira viagem a Washington DC onde se visitaram os monumentos mais importantes da capital dos Estados Unidos, assim como o Capitólio, o Pentágono e o Cemitério Nacional de Arlington.
No final, pode-se afirmar que o curso foi uma excelente experiência a nível profissional e pessoal, tendo

1 http://www.rocketcenter.com/mu/overview

decorrido com muita normalidade e boa disposição, onde se criaram laços de amizade com os elementos do curso, tendo já recebido a visita de dois camaradas americanos ao Porto durante o mês de Janeiro, onde tive a possibilidade de mostrar também um pouco a nossa cultura.



Figura 4 - Visita ao Capitólio (Washington DC)

Arma de Transmissões - Alguma estatística do ano de 2011



TCor Tm (Eng.) Fernando Matos

O presente artigo reúne dados relativos a Oficiais e Sargentos do Quadro Permanente da Arma de Transmissões, que no ano de 2011 viram alterada a sua situação, nomeadamente:

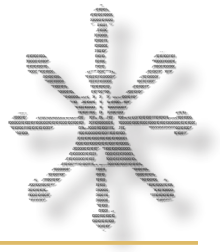
- Ingresso no Quadro Permanente;
- Promoção;
- Passagem à situação de Reserva;
- Abate ao Quadro Permanente;
- Óbitos.

1. Ingresso no Quadro Permanente - Oficiais

TEN TM	12956104	CARLOS ALEXANDRE DA GRAÇA LOPES
TEN TM	08875604	ANDRÁ VICENTE CALVINHO

2. Ingresso no Quadro Permanente - Sargentos

1SARG TM	10862999	HÉLDER RENATO QUEIRÓS COSTA
2SARG TM	13711805	RUBEN TIMÓTEO OLIVEIRA DURÃO
2SARG TM	09879805	MÁRCIA RIBEIRO DA SILVA
2SARG TM	13960306	JOSÉ CARLOS FERREIRA DA SILVA
2SARG TM	06797501	BRUNO RICARDO NEVES MARICATO
2SARG TM	02704904	RICARDO JORGE MAGALHÃES TRIGO
2SARG TM	07310306	JOSE EMANUEL CORREIA FERREIRA
2SARG TM	13279904	ANDRÉ FILIPE ALVES DA COSTA MARQUES
2SARG TM	14073302	ROBERTO JOSÉ ROLO VARAJÃO
2SARG TM	00157606	NÉLSON SIMPLÍCIO ANDRÉ PINHO
2SARG TM	11822605	CHRISTOPHER MANUEL ALVES MONTEIRO
2SARG TM	01291809	ANDRÉ PEREIRA BARBOSA
2SARG TM	07758904	RUBEN RODRIGUES BOTA
2SARG TM	04503909	SUZANA DALILA ALOMAYA MARQUES TAVARES
2SARG TM	00176704	RICARDO MIGUEL RAMALHO PESTANA FIALHO
2SARG TM	14292206	WILSON FILIPE PINTO CARDOSO
1SARG TM	08835301	ANTÓNIO LUÍS PINTO CARVALHO



3. Promoções – Sargentos (demorado)

SAJ TM	1561291	RUI JORGE RIO DOS SANTOS

4. Passagem à situação de Reserva – Oficiais e Sargentos

COR TM	10941478	JOAQUIM CASIMIRO SERÔDIO FERREIRA (1)
MAJ TEXPTM	05372279	HÉLDER JOSÉ MACHADO GONÇALVES
MAJ TEXPTM	12766678	FERNANDO MARQUES DE SOUSA PIRRACO
MAJ TEXPTM	18170074	ANTÓNIO MANUEL SARDINHA VICENTE
MAJ TEXPTM	09911577	MÁRIO PIRES TAVARES
MAJ TEXPTM	19716776	JOÃO JOAQUIM PATRÍCIO LOURENCINHO
MAJ TEXPTM	10077480	VASCO JORGE PINHEIRO CORREIA
MAJ TEXPTM	16408480	JOSÉ MANUEL MONTEIRO
SMOR TM	14925177	DIAMANTINO TAVARES GASPAR
SMOR TM	16033378	FERNANDO COELHO DA COSTA
SMOR TM	06145580	ÁLVARO DOS REIS SANTOS RODRIGUES
SMOR TM	05661379	ANTÓNIO MANUEL DOS SANTOS DOMINGUES
SMOR TM	12543080	ANTÓNIO FERNANDO LAMPREIA CRAVINHO
SMOR TM	16297779	JOAQUIM RODRIGUES DUARTE
SMOR TM	09964480	ANTÓNIO ADÃO BORGES
SMOR TM	07195480	FELICIANO HENRIQUE PAULA DA SILVA
SMOR TM	13377081	ANTÓNIO ABÍLIO ALMEIDA
SMOR TM	03670781	FERNANDO FERNANDES
SMOR TM	00450379	ANTÓNIO GERVÁSIO NUNES DA SILVA MARQUES (1)
SMOR TM	19006981	ARMANDO JORGE DE JESUS APARÍCIO
SMOR TM	12178179	VITOR MANUEL ALVES DE CASTRO
SMOR TM	06387881	ABÍLIO FERNANDES BENTO
SMOR TM	05129682	JOSÉ FERNANDO G. DE FIGUEIREDO SIMEÃO
SCH TM	03118181	DAVID GONÇALVES RODRIGUES
SCH TM	18756284	JOSÉ MANUEL ANDRADE GRILO LOPES DA SILVA
SCH TM	15367182	ANTÓNIO MANUEL CARDOSO BARBOSA
SCH TM	09014284	PAULO HENRIQUE MIRANDA CORDEIRO ALVES
SCH TM	04890984	HÉLDER JORGE RIBEIRO DE OLIVEIRA
SCH TM	07355485	JOSÉ JÚLIO CORREIA FERNANDES BATISTA
SCH TM	06656982	MIGUEL JOSÉ DA COSTA PINTO
SCH TM	06656982	JOSÉ MANUEL CORREIA DE OLIVEIRA
SCH TM	19991684	ANTÓNIO MANUEL DE SEIXAS
SAJ TM	13357685	JÚLIO MANUEL DA SILVA VIEIRA VENÂNCIO
SAJ TM	12647084	MANUEL MÁRIO DOS SANTOS SACRAMENTO
(1) – Na Efetividade de Serviço		

5. Abate ao Quadro Permanente

CAP TM	07509196	PAULO MIGUEL RAMIRES DOS SANTOS

6. Óbitos – Oficiais e Sargentos

COR TM	84082674	JOAQUIM HUMBERTO ARRIAGA DA CÂMARA STONE
CAP TEXPTM	52422011	MANUEL DA SILVA MENDES
2SARG TM	51718411	FERNANDO FARIA DE CARVALHO

Jornadas Técnicas da Arma de Transmissões

As Jornadas Técnicas da Arma de Transmissões, organizadas e coordenadas pela EPT, decorreram de 12 a 13 de Março de 2012, tiveram como finalidade promover o debate sobre vários temas, versando assuntos centrais sobre a Informação, o Batalhão ISTAR, a radiolocalização e o padrão de extensão de segurança em redes, foram abordados ainda temas como a área da formação na Academia Cisco e o e-learning e, por fim, a problemática da Virtualização, tendo em vista a reflexão sobre os temas de uma forma autónoma e da possibilidade de aplicação prática na estrutura do Exército.



TCor Tm (Eng.) João Garcia

As Jornadas Técnicas da Arma de Transmissões foram presididas pelo Exmo. Diretor da Direção de Comunicações e Sistemas de Informação, MGEN Rui Manuel Xavier Fernandes Matias.

O referido evento, organizado em dois dias consecutivos, foi moderado pelo TCor Tm (Eng) João Dias Garcia, Cmdt BTm da EPT.
O Exmo. Diretor da Direção de Comunicações e Sistemas de Informação procedeu à sessão de abertura das jornadas técnicas da arma de transmissões que tiveram início às 10h00 do dia 12mar12.

Os trabalhos foram iniciados com a apresentação do primeiro tema, que teve como orador o Maj Tm (Eng) Carvalho, da DivCSI/EME, subordinado à temática da "Superioridade de Informação". O segundo tema foi apresentado pelo TCor Tm (Eng) Viegas Nunes, Cmdt do BCSI do RTm, cuja intervenção teve como objetivo a "Apresentação do Exercício Ciberdefesa / CiberShield 2012". Seguiu-se um período de debate após cada apresentação, partindo-se posteriormente para o almoço convívio.

No período da tarde, decorreu a apresentação de dois temas, em que os oradores foram o Exmo MGen Xavier Matias e o TCor Inf Varela Cardoso, do CSMIE, que abordaram a questão do "Batalhão ISTAR (Intelligence, Surveillance, Target Aquisition And Reconnaissance)" com duas apresentações, uma sobre o "Sistema de Informação do BISTAR" e a outra subordinada ao tema "O Ciclo de Produção de Informações e o BISTAR", apresentadas pelos oficiais referidos respetivamente, seguindo-se de imediato um período de debate.

Posteriormente, o Ten Tm (Eng) Coelho, 2.º Cmdt na CGE da EPT, apresentou um projeto de radiolocalização denominado "Sistema de Radiolocalização de Emissões Eletromagnéticas" (SRE2), e o Ten Tm Xavier Dias da Secção de Segurança dos Computadores (COMPUSEC) no Centro de Segurança da Informação do RTm, fez uma apresentação versando o tema a "Implementação do Domain Name System Security Extensions (DNSSEC) no domínio <exercito.pt>", seguindo-se um período de debate e, de seguida, o encerramento dos trabalhos do primeiro dia.

No Segundo dia, tiveram lugar duas apresentações que contaram com a participação dos seguintes oradores: o Maj Tm (Eng) Antunes Silva, Chefe do Gabinete de SI na DF da EPT, que apresentou o tema "Academia Cisco - Desenvolvimento e perspetivas futuras", e o segundo orador que foi o TCor Tm (Eng) Ferreira, Cmdt BOAF da EPT, cuja intervenção teve como objetivo a apresentação de um estudo/proposta de "Reestruturação do CFS". Após os períodos de debate foi apresentada, pelo anterior orador, a Engº Ana Dias, da TECMinho, entidade civil convidada que expôs o tema "O E-

Learning no Ensino e na Formação", seguindo-se um período de debate e, por fim, o almoço convívio.
No período da tarde teve lugar a apresentação do tema "Virtualização, o próximo passo" que esteve a cargo do Maj Tm (Eng) Branco, Chefe do Centro de Gestão de Sistemas no BCSI do RTm, seguindo-se um período de debate.

Pelas 16H00 e após o agradecimento por parte do Comandante da EPT, o Cor Tm Rui Manuel Nunes Pinto, da presença e participação de todos os que estiveram presentes nas jornadas da arma, os trabalhos das Jornadas Técnicas da Arma de Transmissões 2012 foram encerrados, tendo presidido à Cerimónia de Encerramento o SubDirector da DCSI, o Cor Tm Tir Pedro Jorge Pereira de Melo.



Figura 1. Mesa de moderação do dia 12mar12



Figura 2. Encerramento efetuada pelo Sub Diretor da DCSI



Já fora da seção de trabalhos foi divulgado informação sobre o blog da História das Transmissões Militares, iniciativa da Comissão da História das Transmissões (CHT), que pode consultado em http://historiadas-transmissoes.wordpress.com/.













ROHDE&SCHWARZ THALES EID