Os Desafios Actuais às Informações Militares

Tenente-coronel
Rui Manuel da Costa Ribeiro Vieira

O conjunto de reflexões apresentadas têm por base a minha experiência no Afeganistão, nomeadamente, no *Counter-Improvised Explosive Device* (C-IED) *branch* do Quartel-General da *International Security Assistance Force* (ISAF), do trabalho realizado na repartição de Informações (G2) da *European Rapid Operational Force* (EUROFOR) e da participação na preparação e na operacionalização do *European Union Battlegroup* 2011-2 (EUBG) da EUROFOR.

Iniciamos com a caracterização genérica dos conflitos actuais com o intuito de identificar o factor que determina esses desafios e desenvolvemos o tema ensaiando em cada momento eventuais soluções práticas ou conceptuais, algumas já efectivas, outras passivas de serem implementadas.

Modelo de conflito actual - O factor indivíduo

O quadro seguinte apresenta os principais factores diferenciadores entre aquilo que era o conflito tradicional e o actual[1].

Modelo Tradicional do Conflito	**Modelo Actual do Conflito**
Estado-Nação vs Estado-Nação	Estado-Nação vs Entidade Não-Estatal
Alianças	Alianças / Coligações / Organizações Internacionais
Hostilidade entre Forças Militares	Hostilidades entre Militares vs Irregulares Polícia vs Terrorista/Criminoso Transnacional
Acções Militares e Policiais independentes	Acção interdependente de todos os recursos de uma Nação ou Organização
Vitória = Fim da campanha decisiva	Vitória = Derrota política do adversário

Vitória = Derrota da força militar adversária	Vitória = Fim das opções/vontade

Examinando os factores constantes do quadro, sem perder de vista a finalidade desta reflexão, isto é, os desafios colocados às IM, destaca-se que nos conflitos actuais onde os possíveis inimigos são entidades não-estatais, organizações rebeldes, insurgentes ou terroristas, dificilmente identificáveis, que actuam no seio dos meios populacionais que lhes conferem apoio e/ou donde recrutam os seus operacionais, o factor INDIVÍDUO passou a estar fortemente presente nos objectivos de qualquer órgão de IM. Este racional é igualmente válido no caso das *Complex Emergencies*[2], que incluem todo o espectro referente a operações de resposta a crises.

Este INDIVÍDUO na maioria das vezes não veste uma farda, tem comportamentos criminais que servem de apoio à sua actuação de base militar, usufrui de apoio da população e/ou de agentes estatais corruptos ou simpatizantes da sua causa e pode estar associado directa ou indirectamente a redes e ameaças transnacionais. Na maioria dos casos é parte integrante do tecido social e cultural onde actua, contrariamente ao caso das forças coligadas que são de natureza expedicionária e operam num ambiente desconhecido, longe das suas origens.

Os inimigos que as forças coligadas enfrentam não integram Brigadas, Divisões ou outras unidades convencionais, constituídas por uma maioria de militares cuja personalidade, poder, autoridade ou influência não são considerados no planeamento das operações. O inimigo de hoje integra uma rede (*network*) de nós com vários graus de interdependência e onde cada INDIVÍDUO tem um peso específico resultante da sua AUTORIDADE, do seu PODER e da sua INFLUÊNCIA. A rede de que falamos tem uma componente física que resulta do contacto directo entre os seus membros e uma componente digital ou virtual que está altamente ampliada pelo uso entre indivíduos, quando disponível, da internet. As IM devem agir sobre estas 2 componentes, sendo que a digital ou virtual é aquela que apresenta maiores dificuldades. Estas dificuldades resultam da necessidade das IM terem necessidade de monitorizar ou, no mínimo, de conhecer os conteúdos do tráfego e dos fluxos de comunicações de indivíduos hostis em plataformas disponibilizadas pelos estados, acessíveis a todos os cidadãos de grande parte do mundo. Este detalhe globalizante faz com que existam, por vezes, questões legais restritivas referentes à violação do direito de privacidade de cada cidadão e exija contactos e troca de informação entre serviços/forças de segurança interna e as IM. Esta colaboração poderá contribuir decisivamente para que as IM identifiquem e localizem estes indivíduos hostis, os avaliem nas suas 3 dimensões[3] para que depois sejam neutralizados através das diferentes e adequadas capacidades das forças coligadas, sejam de natureza letal ou não-letal.

Figura 1 - A construção da rede e a ligação entre as 3 dimensões de cada Indivíduo

Para tornar ainda mais complexa a forma como as IM se devem organizar estruturalmente, que ligações devem estabelecer, de que meios se devem dotar e como devem actuar temos, frequentemente, forças coligadas com missões de base político-militar alargada que têm como objectivos proteger a mesma população de onde este individuo hostil emerge e implementar um Estado de Direito[4], dando especial relevância à implementação e funcionamento do sistema judicial da Nação Hospedeira (NH) onde se trava o conflito. As IM participam neste esforço de proteger a população e apoiar a implementação de um sistema político e judicial funcional onde INDIVÍDUOS são julgados. O General americano David Petraeus, co-autor do recente *Field Manual* (FM) 3-24 *Counterinsurgency* reforça a ideia de que a acção militar nas suas diferentes dimensões deve centrar-se na população. Deve referir-se também que o capítulo das Informações deste manual é o maior de todos e termina com um sumário onde defende que os Comandantes militares devem analisar o inimigo e compreender os aspectos sócio-culturais do Teatro de Operações (TO) donde o mesmo inimigo nasce e se desenvolve.

Este factor INDIVÍDUO constitui-se como o mais relevante e mais actual motor de transformação das IM que força a operacionalização de estruturas, ligações, capacidades e tecnologias capazes de garantir o conhecimento necessário ao processo de decisão militar e político.

O modelo actual do conflito e os desafios às informações militares

Analisando o que foi exposto no número anterior podemos identificar um conjunto de desafios às IM. Iremos abordá-los como se fossem células interligadas que fazem parte de um todo, dinâmico e complexo.

a. Desafio 1 - Integração de capacidades de natureza policial e criminal

Cumprir a missão das forças coligadas nestes ambientes de conflito implica identificar indivíduos que participaram, que participam ou que poderão participar em acções hostis que ameaçam as próprias forças e a paz e a segurança das populações. A identificação de um indivíduo passa pelo reconhecimento visual (nem sempre possível) e/ou pela recolha e reconhecimento dos seus dados biométricos. Tomemos como exemplo o engenho explosivo improvisado (IED), "arma" que isoladamente mais vítimas faz entre a população e entre as forças coligadas no Afeganistão. O IED implica uma rede que abrange o financiador, o comprador e transportador dos materiais que o constituem, o construtor do engenho, o que o coloca no terreno e, em alguns casos, o que acciona o mecanismo. O IED encontrado ou detonado contra uma força militar ou objectivo civil poderá ter, muito

provavelmente, o registo biométrico de alguns destes indivíduos. Será importante a exploração (*exploitation*) do incidente, desde a recolha ao processamento dos elementos de prova.

A recolha imediata ou posterior e o processamento, que poderá e deverá implicar métodos laboratoriais, só deverão ser efectuados por pessoal com as devidas competências e em infra-estruturas especializadas. Estes dados para além de importantes para a força militar podem ser uma ferramenta decisiva para accionar mecanismos legais que credibilizam o sistema político-judicial da HN e em última instância a capacidade da força coligada em cumprir a sua missão. A grande maioria das forças militares ou não possui esta capacidade de investigação policial e criminal que reside nas forças policiais e forças de segurança de natureza militar ou, se a possui é limitada por questões legais nos âmbitos dos seus espectros de actuação. As diversas nações (sobretudo as europeias) que contribuem com forças projectam efectivos policiais muito reduzidos dado que a prioridade desta força é a segurança interna dos seus próprios espaços de soberania. Para além disto a integração de forças policiais e militares numa estrutura única é algo ainda tido como difícil e "constrangedor" pelas duas partes. A solução passa de momento por garantir esta capacidade recorrendo a alguns (poucos) agentes ou forças de segurança de natureza militar, à formação de militares e à contratação de civis e de agentes policiais aposentados que integram estruturas no TO e fora dele (capacidade *Reachback*).

Vejamos o exemplo da estrutura militar americana *COMBINED EXPLOSIVE EXPLOITATION CELL* (CEXC) no Afeganistão. Estas células sob comando militar americano e "*enabler*" da ISAF possuem diversas capacidades de exploração de campo e laboratorial em teatro, recolhem e processam dados biométricos e elaboram relatórios que são difundidos e sincronizados com as IM da ISAF e demais órgãos militares e civis dos EUA. Contribuem decisivamente para a segurança das tropas projectadas e para a integração das seguranças externa e a interna dos EUA.

Department of Defense	US Army Intelligence and Security Command	US Army - National Ground Intelligence Centre
Department of Justice - FBI		International Security Assistance Force Centre

Figura 2 - Algumas Entidades Americanas e Internacionais que partilham Informação recolhida pelas células CEXC

Outro exemplo é o *JOINT PROSECUTION & EXPLOITATION CENTRE* (JPEC), sob

comando militar da *Multinational Force West*, capacidade militar conjunta americana projectada no Iraque, constituída por militares do serviço de Informações dos *Marines*, da *Naval Criminal Investigative Service*, da Força Aérea, por agentes policiais contratados e por intérpretes. A missão desta estrutura é sincronizar as IM e os esforços na consecução de processos judiciais relativos a indivíduos hostis presos e/ou de outro material de prova recolhido no TO.

Figura 3 - Organização do JPEC[5]

Como se poderá verificar pelo descrito e pelas figuras acima expostas, estas capacidades contribuem decisivamente na produção de Informações de níveis táctico, operacional e estratégico.

Os dois exemplos referidos demonstram, implicitamente, que existem grandes desafios no estabelecimento das estruturas fixas e projectáveis, na definição dos canais de fluxo de informação, na aquisição e treino de competências de *Crime Scene Processing*, no manejamento e preservação de elementos de prova, na materialização de investigação laboratorial e no desenvolvimento de prova usável e válida em tribunal.

b. Desafio 2 - Capacidade Permanente de Análise Sistémica

O INDIVÍDUO hostil (inimigo) de que falamos insere-se num AMBIENTE com múltiplas dimensões: social, cultural, religiosa, política, familiar, etc. Em cada dimensão possui determinados de graus de AUTORIDADE, PODER e INFLUÊNCIA que importam analisar. Resulta desta análise holística o conhecimento da posição relativa deste indivíduo no seio da rede e das suas ligações directas e indirectas. Esta situação é francamente diferente quando comparada com a de um ambiente de conflito tradicional centrado em actores estatais, organizações militares e seus líderes políticos, que são previamente identificados e analisados. Actualmente, operacionais e apoiantes hostis (inimigo) possuem grande mobilidade, movem-se entre diferentes aglomerados populacionais, por vezes atravessam fronteiras e entram e saem das diversas redes ao ritmo dos interesses individuais e/ou colectivos. Dado que a ameaça está centrada em INDIVÍDUOS dinamicamente relacionados, isto é, com tarefas interdependentes e fazendo parte de um sistema, de uma rede (que importa conhecer detalhadamente) em que cada elemento afecta os restantes, as IM passaram a ter obrigatoriamente uma abordagem sistémica. Esta abordagem leva a que as forças coligadas tenham hoje um vasto conjunto de

pessoas, estruturas e capacidades de avaliação e interacção com os meios populacionais. Cada uma delas é uma FONTE de PESQUISA e de INFORMAÇÃO com as quais as IM devem interagir. O já referido manual FM 3-24 COIN do General Petraeus afirma que "*All Marines are collectors*".

Por força desta vasta interacção e panóplia de "órgãos de pesquisa" devem surgir e têm surgido *Coordination, Syncronization, Review and Analysis Boards* liderados pelas IM (ex: CJ2) onde têm assento e voz o Conselheiro Cultural, as Operações Psicológicas (PsyOps), o *Civil-Military Cooperation* (CIMIC), as Operações de Informação (InfoOps), etc. Estes *Boards* constituem-se como fóruns importantes de partilha, de recolha e de análise de informação que conduz a um maior conhecimento integrado do AMBIENTE (*environment*) essencial para as avaliações (*assessments*) e produtos das IM. Mas esta interacção deve ser metódica e sistemática, daí resultando a necessidade de adoptar estruturas dotadas dos adequados meios tecnológicos de GESTÃO de INFORMAÇÃO e de CONHECIMENTO. Toda esta informação e todo este conhecimento serão relativamente inúteis se não forem registados e tratados de forma metódica e permanente. Para isso são necessárias bases de dados e sistemas de análise permanentes e poderosos (mesmo ao nível táctico) capazes de correlacionar dados e produzir relatórios de apoio a análises complexas. Isto torna-se decisivo quando temos conflitos de longa duração em que intervêm contingentes militares de diferentes nações com rotações em cada 4, 6 e 12 meses, por exemplo. Neste contexto é tão importante o registo, o arquivamento e o tratamento da informação como a passagem de conhecimento entre contingentes e militares no *Hand Over/Take Over*. A OTAN possui já um conjunto satisfatório destas ferramentas como, por exemplo, o *Battelfield Information, Collection and Exploitation System* (BICES), o *Joint Operations Intelligence Information System* (JOIIS) e outras construídas em teatro (ex: *Counter-IED database* na ISAF). Estes sistemas ou outros equivalentes são uma das vias para que as forças coligadas atinjam a desejada Superioridade de Informação, essencial para a eficácia e eficiência das operações.

Figura 4 - *Battelfield Information, Collection and Exploitation System* (BICES)

Neste capítulo, a União Europeia (UE) tem um caminho mais longo a percorrer devido à ausência destas ferramentas nos *Battlegroups* (BG) aos níveis operacional e táctico. Quando existem são desenvolvidos pelos próprios países que integram os BG, fora do contexto e da liderança do *European Union Military Comitee* (EUMC) *ou Staff* (EUMS), trazendo as esperadas dificuldades de interoperabilidade e de partilha de informação. As coisas complicam-se ainda mais quando os BG integram países membros e não-membros da OTAN que não assinaram acordos necessários para aceder à informação vinda desta organização. Nesta situação poderemos ter forças de um mesmo BG com informação diferenciada mas impossibilitadas de a partilharem formalmente. A UE não possui uma adequada ferramenta de análise sistémica transversal aos três níveis estratégico,

operacional e táctico. Tem no entanto, por via de uma grande integração política, maior facilidade na interacção judicial e policial, facto que não se verifica (em igual modo) ao nível das suas estruturas militares.

Por força da dimensão social e da componente digital da rede, nomeadamente da internet e do seu possível uso por indivíduos hostis, as IM têm perante si um enorme desafio de promover a criação de mecanismos de colaboração com entidades e serviços judiciais e de segurança interna. Estas entidades poderão garantir o conhecimento de conteúdos de comunicações sobre plataformas estatais ou privadas de indivíduos hostis militarmente. Ou seja, se estes indivíduos usarem a internet e os serviços nela disponíveis para coordenarem acções e acederem a conteúdos de apoio à sua acção militar, o conhecimento que corre sobre esta plataforma de comunicação é importante para as IM na dita análise sistémica. Este é talvez o maior dos desafios.

Figura 5 - É fundamental para as IM o conhecimento que flui na componente digital da rede que alimenta a acção hostil de natureza militar

c. Desafio 3 - Partilha de Informação

Os dois desafios anteriores centram-se na capacidade de processar informação enquanto este tem a ver com a informação já processada. Este desafio deriva de factores directamente relacionados com a soberania dos Estados que frequentemente criam limitações à partilha de informação recolhida pelas suas próprias fontes e serviços. Quando pertencem às mesmas organizações (OTAN, UE, etc.) estas limitações reduzem-se substancialmente mas o peso dos interesses de cada nação é sempre determinante no que concerne ao que desejam e permitem partilhar. Devido à natureza dos conflitos modernos este desafio tende a ser cada vez maior e mais complexo, na medida em que, as missões/operações incluem forças militares de diversas organizações e países, organizações não governamentais e organizações internacionais de diversa natureza. As suas participações derivam dos seus compromissos e dos interesses individuais e colectivos que podem ou não ser coincidentes. Vejamos os números de algumas das missões em curso para melhor percebermos a dimensão do desafio. ISAF, 49 nações, 21 das quais não pertencentes à OTAN. *NATO Kosovo Force* (KFOR), 30 nações, 8 das quais não pertencentes à OTAN. *Unified Protector,* 18 nações, 4 não OTAN*. Active Endeavour*, 14 nações OTAN e 2 no programa de *Partnership for Peace* (PfP) e em crescendo. A UE tem também em curso um vasto conjunto de missões militares e civis, algumas delas nas regiões onde se desenrolam as que acima referimos. Esta concentração aumenta ainda mais a complexidade da partilha de informação. São os casos da EULEX no Kosovo, EUPOL no Afeganistão, a EUNAVFOR Atlanta nas águas do corno de África, etc. Se às da OTAN e UE juntarmos as missões da Organização das Nações Unidas (ONU) temos um mapa ainda mais complexo.

Figura 6[6] - Localização de missões militares e civis recentes da ONU, UE e OTAN

Olhando para a figura parece existirem motivos operacionais fortes para que se partilhem informações entre forças e missões que basicamente identificam ameaças equivalentes (ou mesmo coincidentes) e que procuram atingir estados-finais idênticos. Nem sempre assim acontece.

Referimos anteriormente que no seio de uma aliança ou de uma força coligada a partilha está facilitada mas devemos dizer que mesmo aí nem todos os membros têm acesso aos mesmos conteúdos apesar de se verificar o critério da "necessidade de conhecer". Vejamos a ISAF, em 2007/08, no C-IED *branch* um oficial originário de país não pertencente à OTAN, chefe das operações, só tinha acesso á rede *ISAF SECRET* estando vedado aos conteúdos existentes na *NATO SECRET* e no *SECRET INTERNET PROTOCOL ROUTER NETWORK* (SIPRNet) do EUA. Aliás, esta última rede estava apenas disponível para a chamada comunidade dos "*4 eyes*" constituída pelos EUA, Grã-bretanha, Canada e Austrália, deixando de fora todas as restantes nações da ISAF. A mesma informação corria em todos os diferentes sistemas? A dúvida persiste. Ao nível dos BG da UE situações semelhantes poderão ocorrer como aquela que já descrevemos anteriormente.

O problema pode residir nalgumas das seguintes deduções:

- Interesses competitivos entre países e organizações;

- Número reduzido ou ausência de *Fusion Centres*[7] comuns a 2 ou mais países/organizações ou independentes mas colaborantes e comunicantes;

- Ausência de estruturas multinacionais ou multi-organizacionais, de nível político-estratégico, de gestão de órgãos de pesquisa de diferentes origens e de filtragem de grandes quantidades de informação capazes de perceber O QUÊ INTERESSA A QUEM;

- Receio de "fugas" de informação.

Pela natureza dos problemas referidos podemos calcular que dificilmente serão ultrapassados sem serem acompanhados de medidas de integração política e militar, sejam elas de carácter temporário ou permanente.

Os desafios - reflexão conclusiva

Dado a natureza da ameaça nos modernos TO as IM em campanha têm-se centrado também no INDIVÍDUO que tem sido o factor catalisador de parte da sua transformação recente. Este factor tem participado fortemente na geração de um conjunto de transformações e desafios que se centram:

- Na interligação entre a Segurança Interna e a Segurança Externa;

- Na interacção metódica e sistemática das IM com estruturas, entidades e capacidades que são externas à força militar, à organização ou ao país a que pertencem;

- Na integração nas IM de estruturas e capacidades até aqui exclusivas de entidades de natureza policial e criminal (ex: *Crime Scene Investigation*).

Devemos reforçar que este factor INDIVÍDUO revelou que existem motivos operacionais fortes para que se partilhem informações entre forças e missões que basicamente identificam ameaças equivalentes (ou mesmo coincidentes) e que procuram atingir estados-finais idênticos. Tudo passa por, ao nível político, se estabeleçam os acordos, aos níveis estratégico e operacional se criem as estruturas e os fluxos para que ao nível táctico se possam recolher, processar e disseminar a informação de forma a garantir a desejada Superioridade Informação.

Na referida transformação as IM têm-se concentrado no AMBIENTE no sentido mais lato do termo. Este facto tem forçado a que as IM passem a interagir com um conjunto vasto de estruturas e capacidades, de natureza civil, de segurança e de defesa, que possuem informações pertinentes à sua acção. Podemos afirmar que actualmente, decorre uma mudança de paradigma no que concerne às esferas de actuação e interacção entre forças militares dos diferentes ramos, forças policiais e forças de segurança de natureza militar. Esta mudança de paradigma implica mudanças legais, maior integração operacional, treino conjunto e criação de sinergias através do recurso partilhado de estruturas, de pessoal e de mecanismos de processamento de informação. Valerá a pena continuar neste caminho porque terá como resultado um *targeting*[8] mais eficaz, um maior grau de protecção das forças, países mais conhecedores das suas ameaças e riscos e por isso em melhores condições de adoptarem contra-medidas.

Para garantir um todo coerente a transformação tem conduzido a que aos níveis táctico e operacional cada vez maior número das tradicionais estruturas de IM (G2/CJ2) passassem a:
- Liderar fóruns alargados de recolha, de partilha e de análise de informações;
- Munir-se de ferramentas (bases de dados e sistemas de filtragem e de análise) partilhadas com os níveis político e estratégico que permitem uma análise sistémica;

- Garantir a recepção, o registo, o processamento, a partilha e a disseminação de informações com origem em capaciades de *Crime Scene Investigation*.

Figura 7 - Níveis que beneficiam dos contributos da *Crime Scene Investigation* no TO e respectivas áreas onde existe impacto

No entanto, convém referir que os actuais teatros de operações também demonstram que não existem fórmulas únicas e que cada operação tem especificidades que determinam o estabelecimento das IM. O que é basilar é perceber que qualquer processo de decisão se inicia com o que se observa, com o que se conhece, com informação. Qualquer acção, desfasada no tempo em relação ao que se conhecia, incide sobre uma realidade que pode ou não corresponder já à nossa anterior observação. Se a acção incidir sobre a realidade que se conhecia a acção será eficaz, se incidir sobre uma realidade diferente daquela que serviu de base à decisão de agir a acção será desadequada, ineficaz e terá consequências imprevistas no processo de decisão.

Poderemos afirmar, para este efeito, que as IM são decisivas no designado ciclo de Boyd (OODA Loop) constituído por 4 fases: Observar (O), Orientar (O), Decidir (D) e Agir (A). De facto um dos factores de sucesso da acção (Agir) resulta da qualidade, rigor e rapidez da fase da observação (Observar), isto é, dos produtos das IM. A garantia da qualidade dos produtos depende da sua organização, das suas ferramentas de gestão do conhecimento, dos seus órgãos de pesquisa e dos seus fluxos de informação. Tudo isto deve ser permanentemente avaliado a fim de garantir adaptações que derivam da transformação da ameaça e do desenvolvimento da campanha. A geração de forças, onde se incluem os quartéis-generais, para "alimentar" a operação, deve ter em conta estas necessidades de adaptação. Determinado TO pode exigir laboratórios de IED exploitation, outros poderão exigir estruturas de Crime Scene Investigation ou então capacidades e ligações para obter informação do mundo virtual/digital. Mais, nos modernos campos de batalha uma força coligada poderá ter de transitar de operações de combate de alta intensidade para missões de apoio à paz, ou até ter de as realizar simultaneamente. Cada necessidade irá gerar estruturas de IM próprias. Por conseguinte, não se devem adoptar soluções cristalizadas no tempo.

Figura 8 - Ciclo de Boyd - A dimensão Observar das IM: o que observar e como observar.

Por conseguinte, a resposta positiva aos desafios enumerados terá de ser mais ambicioso e abrangente, havendo a necessidade de se constituir como um processo transversal e comum ao conjunto de países e organizações defensores dos mesmos princípios da democracia e da liberdade. Terá de haver um "esbatimento das fonteiras" entre países, no seio das organizações militares, entre estas e entidades de natureza policial e criminal, etc.

Enquanto isto não acontecer, os ditos INDIVÍDUOS que fazem um todo HOSTIL DISPERSO continuarão a poder esconder-se e a operarem nas zonas "escuras" criadas pela falta de integração e colaboração interna e externa do conjunto de países e organizações. A ameaça continuará a ter um leque de opções que alimenta a vontade de continuar a combater!

* Tenente-coronel de Engenharia (Engº). Presta actualmente serviço na EUROFOR.

1 SMITH, Edward A. - Complexity, Networking, & Effects-Based Approaches to Operations, p. 12.

2 Crise humanitária num país, região ou sociedade onde existe uma quebra significativa ou total de autoridade que resulta de um conflito interno ou externo, exigindo uma resposta da comunidade internacional que ultrapassa o mandato ou capacidade de uma única organização ou estado. Definição retirada do Manual *Programme, Policies and Procedures* da UNICEF de 2007.

3 As 3 dimensões: Autoridade, Poder e Influência. Ideia adaptada da apresentação *The Importance of Cultural Understanding*, do Prof. Dr.Patrick Sookhdeo, professor convidado da NATO school - Curso M3-50-B11 *Peace Support Operations.*

4 Na maioria dos casos de padrão ocidental.

5 http://publicintelligence.net/joint-prosecution-and-exploitation-center. Acedido em 23/10/11.

6 Retirado da apresentação *Tensions and Challenges* do Coronel Peter Schneider, professor convidado da *NATO School* - Curso M3-50-B11 *Peace Support Operations.*

7 *Fusion Centre* pode ser definido como sendo uma estrutura de colaboração entre 2 ou mais entidades que partilham recursos, competências técnicas e/ou informação (INTEL) com o objectivo de maximizar a capacidade de compreender, detectar, prevenir ameaças e, consequentemente, apoiar medidas de natureza diplomática, política, judicial, militar ou policial. Adaptado do documento *Fusion Centre Guidelines* dos Departamentos de Justiça e Segurança Interna dos EUA, 2005.

8 Definição de *Target*: Área geográfica, objecto, organização, complexo, instalação, unidade ou pessoa sobre a qual está planeada uma acção de vigilância, investigação, neutralização ou destruição por meios militares. O *Targeting* constitui-se como o processo que inclui todos os passos do planeamento e da acção de capacidades militares de natureza letal e nao-letal.