VII CONGRESSO PORTUGUÊS DE SOCIOLOGIA
19 a 22 Junho 2012
Universidade do Porto - Faculdade de Letras - Faculdade de Psicologia e Ciências da Educação
SOCIEDADE
CRISE E RECONFIGURAÇÕES

ÁREA TEMÁTICA: ST9 – Segurança, Defesa e Forças Armadas

CONTRATERRORISMO: O PAPEL DA *INTELLIGENCE* NA ACÇÃO PREVENTIVA E OFENSIVA

MATOS, Hermínio
Doutorando e Mestre em História, Defesa e Relações Internacionais (ISCTE-IUL/AM)
Investigador e Docente do ICPOL – ISCPSI
hjmatos@psp.pt

Resumo

A eficácia concertada que os ataques terroristas perpetrados em Setembro de 2001 nos EUA lograram alcançar, foi responsável pelas reformulações operadas, posteriormente, nas estruturas de segurança e de defesa de grande parte dos Estados Ocidentais. Estas reformulações resultaram da (re)configuração da própria ameaça: exponencialmente letal, de implantação difusa e carácter imprevisível, logrando dificultar a prossecução de quaisquer estratégias contraterroristas até então implementadas contra o terrorismo internacional. As experiências ocidentais até então ditadas pelo "terrorismo doméstico" privilegiavam, quase sempre, uma abordagem contraterrorista de pendor reactivo. No actual "quadro de ameaças", porém, julgamos que a resposta contraterrorista necessita de operar activamente na área da *Intelligence*, promovendo a infiltração de células ou grupos terroristas que se constituam como fontes de ameaça à segurança internacional. Falamos, em concreto, da dinâmica – estratégica e operacional – que envolve a "manobra de infiltração", ou penetração, de organizações terroristas, especialmente as conotadas com o terrorismo internacional de matriz islamista, no âmbito da actividade dos serviços de informações ou das forças policiais. Só através deste tipo de acção se pode obter informação privilegiada que permita prever ou anular o curso de uma acção terrorista, permitindo desencadear os mecanismos de prevenção e resposta adequados.

Abstract

The effectiveness of concerted terrorist attacks occurred in 2001 in the U.S. homeland have achieved, was responsible for reformulations operated later in the security structures of Western States. These restatements were the result from the reconfiguration of the threat itself, exponentially lethal, by their diffuse and unpredictable deployment, managing to hinder the pursuit of any counterterrorism strategy implemented so far against international terrorism. The Western experience so far dictated by the "domestic terrorism" privileged, often, a bias for reactive counterterrorism approach. Under the current "picture of threats," however, we believe that the counterterrorism answer needs to operate actively in the field of intelligence, promoting the infiltration of terrorist cells or groups that constitute as sources of threat to international security. In particular, the dynamics - strategic and operational - involving the "infiltration maneuver", or penetration of terrorist organizations, especially international Islamic terrorism within the activities of intelligence agencies or forces police. Only through this type of action can be obtained inside information that allows to predict or reverse the course of terrorist action, allowing the trigger mechanisms of prevention and appropriate response.

Palavras-chave: Contraterrorismo; Intelligence; Infiltração; Preventiva; Ofensiva;
Keywords: Counterterrorism; Intelligence; Infiltration; Preventive; Offensive;

[PAP 1146]

Contraterrorismo: o papel da *Intelligence* na acção preventiva e ofensiva

Nota: A responsabilidade das ideias vertidas no presente artigo reflectem, exclusivamente, as opiniões pessoais do seu autor, formuladas numa perspectiva académica, e não vinculam, no todo ou em parte, a Instituição Policial à qual o autor se encontra vinculado profissionalmente.

Introdução

Os ataques terroristas perpetrados em 11 Setembro de 2001, nos EUA, assumiram um papel determinante nas reformulações operadas, a partir de então, nas estruturas de segurança e defesa de grande parte dos Estados Ocidentais. Tais reformulações, no entanto, resultaram também da reconfiguração da própria ameaça: exponencialmente letal, de implantação difusa e carácter imprevisível, dificultando, se não mesmo anulando, a prossecução de estratégias de prevenção e resposta até então implementadas contra o terrorismo internacional, em especial aquele gizado pela al-Qaeda e pela "nebulosa terrorista" a ela directa ou indirectamente associada, através dos seus grupos afiliados, autoproclamados afiliados e células locais ou indivíduos isolados, fenómenos emergentes e agora denominados, respectivamente, de "home-grown" e "lone-wolf" terrorismo (Matos, 2011).

As experiências ocidentais até então ditadas pela acção do "terrorismo doméstico" privilegiaram, quase sempre, uma abordagem contraterrorista de pendor reactivo. No actual "quadro de ameaças", todavia, a resposta contraterrorista deve ser fortemente sustentada pela área de actuação da *Intelligence* – em especial na área da pesquisa e recolha de informações através de fontes humanas – promovendo a infiltração de células ou organizações terroristas que constituam ameaça, potencial ou efectiva, à segurança internacional.

A acção preventiva da *Intelligence* incide, no essencial, na pesquisa, recolha e análise de informações sobre indivíduos/células/grupos cujas acções se relacionem com actividades de incitamento, apoio, propaganda, radicalização violenta ou recrutamento terrorista – ou actividades criminosas que sirvam de suporte à acção terrorista, amiúde denominados "crimes instrumentais" do terrorismo – e ainda a constante monitorização e avaliação da ameaça.

A vertente ofensiva, por seu turno – e uma vez já identificado o "foco de ameaça"[1] –, pode actuar em dois grandes vectores:

1) Apoio ao planeamento operacional e intervenção táctica de Forças e Serviços de Segurança ou, quando aplicado[2], do instrumento militar.

2) Acção encoberta, na área do HUMINT[3], nomeadamente através da infiltração ou penetração de células ou organizações terroristas e na gestão, controlo e manipulação de fontes humanas de informação.

Um princípio basilar da "recolha clandestina" de informações através de fontes humanas – uma vez que estas também podem provir de fontes abertas e por métodos não cobertos de pesquisa e recolha – é de que este instrumento só deve ser aplicado como último recurso e após avaliada a sua possibilidade de sucesso (MacGaffin, 2005, pp. 80-81).

Destarte, impõe-se uma análise à dinâmica – estratégica, operacional e táctica – que envolve a "manobra de infiltração", ou penetração, de "agentes" em células ou organizações terroristas, especialmente as conotadas com o terrorismo internacional de matriz islamista.

No caso concreto do terrorismo de matriz islamista, o processo de infiltração torna-se mais difícil de gizar, dadas as assimetrias culturais, religiosas e linguísticas que se verificam. Neste sentido, impõe-se uma análise dos diversos estádios do processo de infiltração: da captação à desactivação (ou "exfiltração") do agente de infiltração.

A história recente do contraterrorismo internacional tem demonstrado que nesta área de actuação, é análogo o *modus operandi* de serviços de informações e de organizações terroristas, podendo estabelecer-se entre a *Intelligence* e o Terrorismo uma relação de "gémeos siameses" (Todd *et al*., 2004, pp. 12-13), expressa numa aparente relação causal, e interdependente, entre a intensificação da acção contraterrorista de um Estado e o aumento – em contra-resposta – do número de ataques perpetrados por uma organização terrorista, fenómeno a que Ganor (2005) designou por "efeito boomerang".

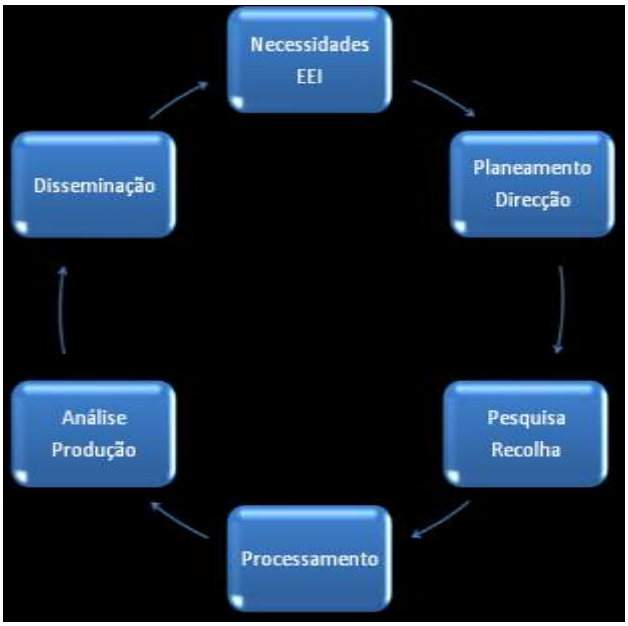
1. Contraterrorismo e *Intelligence*

É, pois, um lugar-comum evocar os ataques terroristas de 11 de Setembro de 2001 como um marco diferenciador na Nova Ordem Mundial. Porém, este evento apenas logrou imprimir alterações significativas nas agendas dos Estados Ocidentais em matérias concernentes às suas políticas de segurança e defesa. Igualmente importante, também, foi a consciencialização generalizada de que nenhum Estado – independentemente da sua hegemonia económica ou poderio militar – poderia, de forma isolada, fazer face a uma ameaça como a configurada pelo terrorismo internacional, especialmente aquele que se relaciona com a al-Qaeda.

A implosão da União Soviética, em 1991, promoveu, assim, alguma inépcia nos departamentos responsáveis pela pesquisa e recolha activa de informações através de fontes humanas[4] –HUMINT –, reflexo também do desenvolvimento exponencial dos meios técnicos[5] de recolha de informações e, em particular, da pesquisa destas em fontes abertas de informação[6], conduzindo, inexoravelmente, aos habitualmente denominados *Intelligence Failure*, alguns dos quais acabariam por "facilitar" a concretização, bem sucedida, dos ataques terroristas perpetrados, posterior e sucessivamente, em Nova Iorque e Washington, em 2001, em Madrid, em 2004, e em Londres, em 2005 (Matos, 2011, p. 4).

Com o fim da Guerra Fria, "both the policy-makers and the intelligence agencies scanned the horizon for new enemies and failed to spot the emergent threats (…) this contributed to a downsizing of human intelligence activities, precisely the kind of capability that is most important in the context of counter-terrorism" (Andrew *et al.*, 2009: p.160), criando-se assim um "*vacuum*" na definição, implementação e agilização das políticas de segurança nacional (Berkowitz *et al*., 2000, p. 3).

No âmbito do presente artigo, a *Intelligence* é, conceptualmente, formulada de acordo com a sua perspectiva tridimensional, ou seja: 1) a *Intelligence* como **processo** – de planeamento, pesquisa e recolha, processamento, análise e produção, visando determinados objectivos; 2) a *Intelligence* como o **produto** final desse processo – "*That kind of Knowledge*" preconizado por Kent[7]– e que, uma vez difundida pelos canais próprios, se constitui como precioso instrumento de apoio à decisão, ao nível estratégico ou operacional; e 3) a *Intelligence* do ponto de vista – estrutural e funcional – das **organizações** que a executam (Lowenthal, 2006, p. 9).



Esquema 1: O "Tradicional" Ciclo de produção de Informações
Fonte: elaboração própria, Cf. Clark (2007)

De acordo com o esquema anterior, o "ciclo tradicional" de informações releva para um processo de produção que, embora dinâmico, se mostra por vezes demasiado linear. Nessa perspectiva, Clark (2007, pp. 8-25) preconizou o "*Target-Centric Approach*", modelo cuja ênfase releva para um ciclo de produção de informações não só centrado no alvo como, simultaneamente, envolvendo todos os seus actores (i.e., decisores, agentes de pesquisa, analistas, programadores, tradutores, etc.) e assente num ciclo dinâmico, mas não linear, e configurado em rede.

O contraterrorismo, como a estratégia de acção/resposta de um actor estatal, compreende as medidas destinadas a prevenir, ou mesmo anular, o fenómeno a montante da acção terrorista. É a componente pró-activa que contempla, *inter alia*, a infiltração de redes ou células terroristas e a pesquisa e recolha activa de informações através de HUMINT (Baud, 2005, p. 298).

Frequentemente, parece subsistir uma divergência conceptual entre este conceito e um outro – frequentemente usado, de modo oposto ou alternado – que é o de antiterrorismo. Este último parece identificar-se, muito mais, com a componente de actuação centrada, por um lado, na "protecção" (na perspectiva passiva)[8] e, por outro, na vertente reactiva, isto é, uma vez consumada, com êxito, uma acção terrorista.

A doutrina militar norte-americana define separadamente ambos os conceitos: antiterrorismo, como "as medidas defensivas destinadas a reduzir a vulnerabilidade de pessoas e bens a ataques terroristas"; contraterrorismo, como as "medidas ofensivas destinadas a prevenir, impedir e responder ao terrorismo" (Joint Chiefs of Staff, 1993, p. I-1).

Julgamos, no entanto, que essa divergência conceptual radica muito mais num confronto de natureza semântica, suprida hoje pelo uso generalizado do termo "contraterrorismo", o qual integra, independentemente da sua perspectiva operacional ou especificidade linguística, ambos os vectores – de prevenção, pro-acção e resposta – em qualquer das suas fases (Matos, 2012b).

2. O espectro da *Intelligence* no contraterrorismo

O espectro de actuação da *Intelligence*, na perspectiva contraterrorista, pode, simultaneamente, abranger vectores de intervenção nas áreas preventiva e ofensiva, a saber:

- *Pesquisa e recolha,* aberta e encoberta, processamento *e análise de informações* sobre a envolvente da ameaça terrorista, com vista a uma *Comphreensive Approach* ("Big Picture") do fenómeno.

- *Captação, recrutamento, treino e gestão de fontes humanas de informação* (redes de "agentes", informadores, contactos, etc.).

- Análise, estratégica e operacional, de informações relacionadas com o terrorismo, como instrumento de apoio à decisão e à intervenção operacional e táctica das FSS. Numa analogia com o conceito de *Intelligence-Led Policing*[9], um "*Intelligence-Led Counterterrorism*".

- *Processamento de informações provenientes de outras FSS*, especialmente no que se refere a grupos ou organizações criminosas que se dediquem à prática de crimes instrumentais do terrorismo.

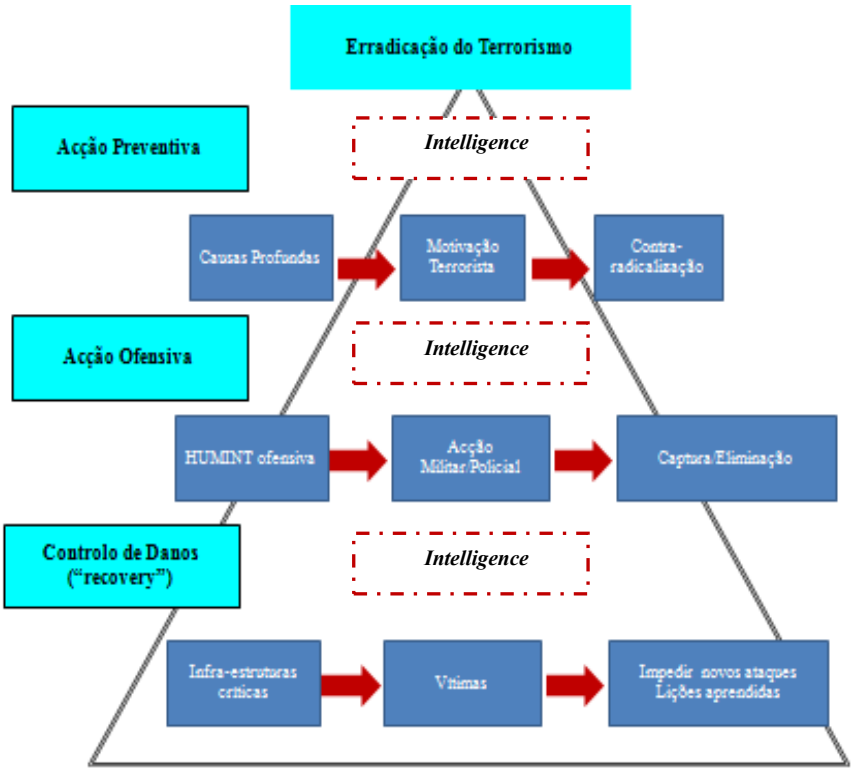
- Criação de *Sistemas de Alerta Precoce* contra a ameaça terrorista, a chamada *Early Warning Intelligence* (EWI), com vista à caracterização e avaliação da ameaça terrorista.

- *Contra-informação*[10] na área do terrorismo, em especial detectando actividades de *Intelligence* (recolha de informação, vigilância e contra-vigilância, ensaios de segurança de alvos, etc.) por parte de células ou grupos terroristas em território nacional.

- *Cooperação internacional* na área das informações relativas ao fenómeno terrorista.

- *Avaliação de risco e grau de ameaça de alvos específicos*:
  - Alvos humanos, possibilitando o reforço da sua protecção ou mesmo a sua "transferência".
  - Infra-estruturas críticas ou simbólicas.
  - Grandes eventos, cimeiras políticas, etc.
  - Capacidades, intenções e grau de ameaça relativamente a indivíduos, células ou grupos terroristas, ou outros com estes directa ou indirectamente relacionados em actividades de apoio logístico e/ou operacional.
  - Identificação e monitorização de indivíduos/células e/ou locais conotados com actividades de recrutamento e radicalização violenta.

Nesta perspectiva de concretização, a *Intelligence* é pois transversal a todo o espectro da resposta ao fenómeno terrorista, independentemente da área e do nível de intervenção em que nos situemos, tal como ilustra o Esquema seguinte (Esquema 2).



Esquema 2: Objectivos estratégicos numa política Contraterrorista
Fonte: elaboração própria, de acordo com Ganor (2005, p. 26)

No âmbito da acção preventiva, é essencial que uma análise das causas profundas do fenómeno – de cariz estrutural – seja efectuada em toda a sua extensão e profundidade. Também a análise dos factores precipitantes ("trigger causes"), enquanto eventos de natureza conjuntural que precedem, e contextualizam, a imediata ocorrência do fenómeno terrorista, é de importância vital.

Tendo em conta a "equação terrorista", cuja fórmula estabelece que "o terrorismo é o somatório da motivação e capacidade operacional do grupo ou organização" (Ganor, 2005, p. 42), resultando um incremento da acção terrorista na razão directa do aumento do índice de cada uma das variáveis, impõe-se uma actuação nesta área, contemplando ambas as vertentes, por forma a reduzir a motivação e a capacitação de recursos (humanos e logísticos) do grupo ou organização.

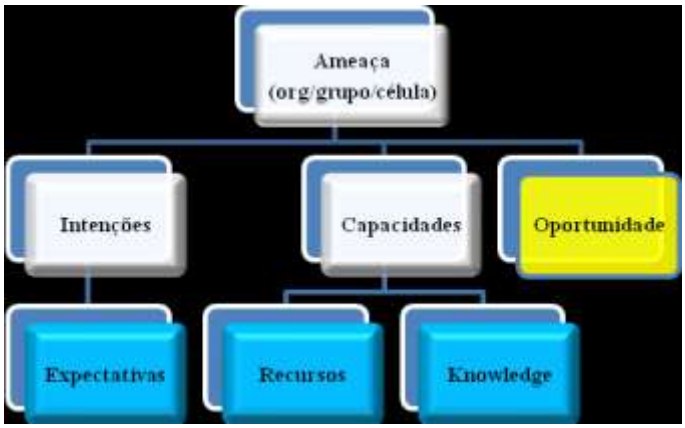
No vector de intervenção durante ou após o incidente – essencialmente de contenção e controlo de danos – o reforço e reavaliação da protecção de alvos críticos, previamente identificados e submetidos a análise de risco e do grau de ameaça, deve ser efectuada e mantida, até porque um ataque terrorista pode ser seguido de outros ataques, em simultâneo ou sequenciais. Não raras vezes, o primeiro ataque é apenas uma manobra para focalizar, num determinado ponto, a acção das forças e serviços de segurança, protecção e socorro (no denominado "efeito de túnel"), conduzindo assim à diminuição do grau de protecção de outros alvos críticos – por deslocação e concentração das forças no local do primeiro incidente – o que facilitará a acção terrorista para a consecução de novos ataques, quase sempre de maior impacte.

3. A acção Preventiva da *Intelligence*

Um dos problemas com que a *Intelligence* se confronta no amplo espectro da sua intervenção contraterrorista é a natureza clandestina e o carácter hermético que reveste a estrutura, funcionamento e acção de uma célula ou organização terrorista, pelo que a sua penetração ou infiltração é especialmente difícil de concretizar. Desse modo, o conhecimento prévio, ou atempado, do planeamento de um ataque terrorista fica mais longe de ser alcançado através de uma acção de *Black Intelligence*[11].

O vector preventivo da *Intelligenc*e assenta, em grande medida, na capacidade de interacção e correlação entre cada um dos protagonistas que integram o ciclo de produção de informações em toda a sua extensão e profundidade, independentemente das especificidades inerentes a cada uma das suas fases, devendo apresentar-se como um produto final cujas consequências – no seu todo, mais do que a soma de cada uma das partes – se traduzam em "conhecimento" útil, e oportuno, de apoio à decisão.

Um exemplo de falhanço de interacção, integração e correlação de cada um desses vectores pode ser percebida na explanação seguinte: "In the mission to provide a usable warning, performance before September 11 failed in all phases of the intelligence cycle. The system failed in collection, since it did not discover the perpetrators, plans, or means of attack (…). It failed in processing and dissemination, as some pieces of information were not correlated in ways that would have raised the odds of identifying individuals involved in the plot or the instruments they planned to use. It failed in analysis by not finding the right pattern by which to connect the dots within the array of clues that was both incomplete and full of clutter" (Betts, 2007, p. 105).



Esquema 3: Modelo de Análise para indicadores e potencial da ameaça terrorista

Fonte: elaboração própria, de acordo com Torres (2009, pp. 54-55)

4. A acção Ofensiva da *Intelligence*

As limitações, ainda que pontuais, de cada um dos instrumentos disponíveis na luta contra o terrorismo faz com que seja necessário – ou pelo menos considerada – a hipótese do seu uso alternado ou cumulativo. Independentemente da especificidade ou tipologia da estratégia contraterrorista adoptada, em qualquer delas a *Intelligence* é uma peça fundamental (Pillar, 2003, p. 123). Não existe uma fórmula consagrada, e universal, para uma estratégia contraterrorista, dada a heterogeneidade, quer do fenómeno em si, quer de cada um dos actores em confronto. Existe, ainda assim, a tipificação de alguns "modelos" contraterroristas, de acordo com as propostas de dois especialistas, e que passamos a enunciar:

Crelinsten (2009), por exemplo, divide o espectro contraterrorista em cinco grandes variantes: *coerciva*, *proactiva*, *persuasiva*, *defensiva* e de "*longo prazo*". Dado as limitações gráficas do presente artigo, apenas nos ocuparemos da variante coerciva, dado ser a que, directa e mais vincadamente, se relaciona com a acção ofensiva da *Intelligence*.

Assim, sob a égide da variante coerciva são erigidos dois grandes modelos contraterroristas:

1) O "Criminal Justice Model", em que "counter terrorism treats terrorism as a crime. This makes perfect sense, since most terrorist acts constitute crimes defined in criminal codes." (Crelinsten, 2009, p. 52). Neste modelo, a resposta ao fenómeno terrorista resulta da acção convergente, e complementar, das Forças e Serviços de Segurança, do sistema judiciário e penal e, tal como no caso do modelo seguinte, do papel preponderante e subsidiário da *Intelligence* (aqui, não só no âmbito dos serviços de informações propriamente ditos, mas igualmente das informações policiais/criminais, no âmbito da actividade policial de prevenção e investigação criminal).

2) O "War Model", no qual "counterterrorism treats terrorism as if it were an act of war or insurgency. Because wars are usually fought between states, countering terrorism within a war model implies that the terrorist group represents the equivalent of a state." (Idem, pp. 72-73) ou seja, tem primazia o emprego do instrumento militar. São exemplos paradigmáticos do uso deste modelo os casos dos EUA e de Israel.

Na perspectiva de outro especialista, a definição de qualquer política contraterrorista deve procurar dar resposta a três grandes objectivos:

1) a eliminação do terrorismo;

2) a minimização dos danos causados pela acção deste; e

3) prevenir a escalada da acção terrorista (Ganor, 2005: pp. 25-27).

Em ambos os casos, porém, os efeitos de uma acção iminentemente ofensiva podem resultar paradoxais: é o dilema que reveste aquilo que poderíamos designar por "equação contraterrorista", no sentido em que, paralelamente ao incremento de uma acção ofensiva que vise reduzir as capacidades de acção de um grupo ou organização, corresponderá o aumento dos seus níveis de apoio, adesão e motivação para a prossecução da acção terrorista, traduzidos quase sempre numa escalada do número de ataques e, não raro, do seu impacte.
Deste modo, uma estratégia contraterrorista deve procurar o equilíbrio entre os meios destinados, por uma lado, a anular a capacidade operacional de uma organização para a actividade terrorista, por outro, reduzir, ao mínimo, os níveis de motivação para a sua consecução (Matos, 2012b).

5. A Infiltração Contraterrorista

O processo de infiltração numa estrutura terrorista visa, em última análise, a obtenção de informações a partir de fontes humanas, ou seja, de agentes previamente "recrutados" por um serviço e sob o controlo[12] e supervisão de um oficial de informações.
A actividade da *Intelligence* no contraterrorismo persegue, assim, o primado da prevenção terrorista: a identificação e localização, oportuna, de uma célula ou grupo, bem como as suas actividades de planeamento, preparação e execução de um ataque terrorista.
Uma resposta adequada não é necessariamente apenas aquela que anula por completo a ocorrência do evento, através da localização e detenção de uma célula ou grupo. Nalguns casos, e mercê das informações disponíveis, o reforço de segurança de um alvo, a redução dos seus níveis de vulnerabilidade ou a sua transferência permitirão, igualmente, minimizar as hipóteses de concretização de um ataque ou, no mínimo, mitigar os seus efeitos.
A grande valência da *Intelligence* no contraterrorismo é, pois, a de recolher e disponibilizar informação sobre indivíduos, líderes, células ou grupos terroristas, por forma a facilitar o seu desmembramento. Simultaneamente, é também "o de saber assinalar pontos de viragem na forma como as ameaças se colocam; percepcionar o embrião de novos grupos terroristas; a alteração do *modus operandi*, de cariz mais violento." (Rego, 2007 e 2010).
No que concerne ao uso de "agentes" de infiltração ou à penetração de alvos terroristas, as informações – se aqui perspectivadas já como um "produto acabado" – são tanto mais valiosas (dada a sua precisão, oportunidade e disponibilidade) quanto maior a proximidade da fonte, ou agente de infiltração/penetração, relativamente à origem, ou seja, ao alvo.

Importa diferenciar, em termos conceptuais, "infiltração", que se opera de fora para dentro, da "penetração" de um alvo, que é conseguida quando um elemento que já pertence à estrutura organizativa desse alvo, ou com este tem relações funcionais ou de acesso privilegiado, se dispõe a fornecer informações a partir do seu interior. Ou seja, a abordagem do alvo e a dinâmica da acção, neste último, é feita de dentro para fora.

O processo de infiltração, cujo desenho pode assumir processos mais ou menos elaborados, de acordo, antes de mais, com a complexidade do alvo de infiltração, é uma "imbricada amálgama de influências, relações e processos que fazem das operações de infiltração exercícios onde a planificação, as componentes de acção e a sua aplicação se convertem em desafios de precisão para agências e serviços de informações" (Gómez, 2007, p. 3).

No esquema seguinte (Esquema 4) ilustram-se alguns dos estádios do processo de infiltração, sendo que a nossa perspectiva é apenas consagrando o "agente" como o que actua sob controlo e direcção de um oficial de informações e não sob a possibilidade – nalguns países legalmente consagrada – de essa figura ser preenchida por um funcionário das forças ou serviços de segurança.

Até porque, convenhamos, na área do combate ao terrorismo, e em especial o de matriz islamista, essa infiltração não só era demasiado arriscada em termos de segurança do funcionário, como a imersão num ambiente de prática criminosa continuada colocaria, *a posteriori*, inúmeras questões legais.

Por último, mas não menos importante, uma infiltração de duração mais longa ("deep cover") como aquela que se afigura necessária à infiltração de uma estrutura terrorista, requer a criação de uma "lenda"[13] mais elaborada e uma imersão na "identidade" mais profunda e duradoura. Em resultado, após a exfiltração do funcionário e no processo de "desactivação", quer o retorno à sua identidade, quer a reinserção no meio social e familiar não estarão isentos de problemas de índole psicológica.

Esquema 4: Fases do Processo de Infiltração Contraterrorista
Fonte: Elaboração própria, adaptado de Gómez (2007, p.7)

De forma sucinta, analisemos cada uma das fases do processo de infiltração:

Recrutamento – O processo de recrutamento de um "agente" – desenvolvido por serviços de informações, no âmbito da sua actividade, ou por organizações policiais, em sede de investigação criminal – inicia-se com o estabelecimento de um determinado objectivo ou missão. Para a infiltração de um alvo como um grupo ou organização terrorista, o recrutamento é feito de acordo com o perfil adequado[14], previamente estabelecido, de entre os potenciais "alvos" de recrutamento. Para o estabelecimento deste "perfil", e consequente "elegibilidade" do alvo, concorrem inúmeros factores, sendo os mais importantes, entre outros, as características físicas e psicológicas do alvo, o seu grau de acesso à estrutura ou informação que se pretende alcançar e o seu grau e tipo de "motivação"[15].

Formação e Treino – Nesta fase, pretende-se que o "agente adquira ou reforce algumas competências operativas, essencialmente em três áreas de formação: psicológica, instrumental e profissional. A primeira, visando o enquadramento sustentável, do ponto de vista psicológico e social, do agente no ambiente de infiltração, conferindo-lhe ainda, entre outras, capacidades de comunicação e persuasão, dissimulação e engano, instrumentos extremamente úteis à gestão das relações interpessoais que será obrigado a desenvolver e manter no âmbito da sua acção. As duas últimas vertentes, são ajustadas em função dos objectivos e duração da manobra de infiltração, da especificidade do alvo e integrando competências operacionais, linguísticas, culturais, etc. (Gómez, Idem, pp. 12-13).

Imersão – é *o capítulo mais complexo do processo de infiltração*. A imersão está programada para estabelecer, configurar e implantar uma identidade, física e psicológica, fictícia num agente de infiltração. O processo de imersão persegue dois objectivos primordiais: por um lado, confirmar o grau de incorporação da identidade por parte do agente; por outro, verificar a eficácia da sua representação. Paralelamente, permite isolar e manter intactos os elementos constituintes da sua identidade própria, evitando contudo que estes se imiscuam na aplicação dos elementos psicológicos da identidade agora assumida.
Embora intrinsecamente ligada à componente operativa do processo de infiltração, esta é uma fase que requer uma monitorização constante por pessoal especializado (Gómez, *Ibidem* e Matos, 2011).

Infiltração – Concluídas as fases precedentes, capacitação e imersão, segue-se a manobra de infiltração do agente no contexto operacional em que irá actuar. Esta acção pode ser executada de forma isolada ou integrada[16], de acordo com o perfil criado para o agente e atento as especificidades do alvo. A acção de infiltração, em nosso entender, tem início com o momento de contacto directo do agente com a estrutura ou organização a infiltrar e percorre um *continuum* que termina, apenas, com a exfiltração do agente (Matos, 2011, p. 56).

Controlo ou "handling" – Esta fase do processo é desempenhada exclusivamente através do "agente de contacto" ("handler") e integrará a consecução de quatro objectivos: cobertura do agente infiltrado, recolha de informação, (re)orientação das condutas e procedimentos tácticos do agente infiltrado, visando lograr uma maior segurança e eficácia operativa, e apoio psicológico, visando mitigar os efeitos negativos da clandestinidade (Matos e Gómez, *Ibidem*).
As formas de contacto entre o agente infiltrado e o seu *handler* estão devidamente implementadas, exaustivamente previstas e testadas na fase de planeamento da operação, e contemplando inclusive outras formas de contacto alternativas.
Um acompanhamento psicológico permanente, quer do agente infiltrado, quer do seu *handler*, sempre que possível, permitirá detectar precocemente quaisquer sinais de stress ou outros comportamentos que ponham em causa o sucesso da operação e a segurança dos seus intervenientes (Gómez, p. 14).

Exfiltração – Uma missão de infiltração pressupõe, desde logo, um plano de exfiltração. O seu planeamento deve estar concebido desde a fase inicial de planeamento, dado que a qualquer momento, e pelos motivos mais díspares, pode ser necessário proceder à extracção do agente infiltrado. Neste sentido, esta é uma acção táctica que ocorre, não apenas quando é dada por finda a missão de infiltração, conseguidos que estão os objectivos desta, mas também de forma inopinada, por razões de comprometimento de segurança do agente ou ineficácia da operação (Matos, 2011, p. 57).

Reinserção ou "desactivação" - Mais não é que a "devolução" da verdadeira identidade, e o acompanhamento, a todos os níveis, na reintegração deste ao seu ambiente pessoal, social e profissional (*Ibidem*, p. 58).

6. Síntese Conclusiva

As potencialidades da *Intelligence* na resposta ao fenómeno terrorista actual – em especial o gizado pelo al-Qaeda e Movimentos Associados (AQAM) – ficaram expressas na sua dupla e complementar vertente de actuação: a montante da acção terrorista, no âmbito da prevenção e avaliação da ameaça, em especial através da recolha de informações, e monitorização, de indivíduos ou estruturas terroristas e na criação de sistemas de alerta precoce; a jusante da acção terrorista, como instrumento de apoio à acção contraterrorista ofensiva, em especial na condução de operações militares ou policiais – de captura ou eliminação de alvos terroristas (obviamente que nos referimos a estratégias contraterroristas de países como os EUA, Israel ou mesmo a Rússia), em especial de alvos de "elevado perfil" – e ainda na condução de operações HUMINT, de pesquisa e recolha de informações, em especial as tão necessárias manobras de infiltração ou penetração de alvos terroristas, único meio de obter informações, actualizadas e oportunas, sobre o planeamento, preparação ou execução de um ataque terrorista.
Só deste modo é possível obter informação "privilegiada" que permita, em última análise, prever ou anular o curso de uma acção terrorista e, desse modo, desencadear os mecanismos de resposta adequados.
"***Counterterrorism is an intelligence war***. The intelligence community plays a central role in counterterrorism in at least three key ways: 1) understand the threat; 2) give warning of adversaries' intentions and capabilities; and 3) find and disrupt the adversary" (Pollard, 2009, p. 117). Concordamos com Pollard, se bem que, como em qualquer Guerra, também nesta algumas batalhas (ainda se) perdem…

Bibliografia

Baud, Jacques (2005), *Le Renseignement et la Lutte Contre le Terrorisme*. Paris: Lavauzelle.
Berkowitz, Bruce D. *et al.* (2000), *Best Truth, Intelligence in the Information Age*. New Haven: Yale University Press.

Betts, Richard K. (2007), *Enemies of Intelligence, Knowledge and Power in American National Security*. New York: Columbia University Press.

Clark, Robert M. (2007), *Intelligence Analysis: a Target-Centric Approach.* Washington: CQ Press.

Crelinsten, Ronald (2009), *Counterterrorism.* Cambridge: Polity Press.

Denécé, Éric (2008), *Renseignement et Contre-Espionnage. Actions Clandestines, Technologies, Services Secrets*. Paris : Hachette.

Desmaretz, Gérard (2007), *Le Renseignement Humain*. Paris : Chiron Éditeur.

Dulles, Allen W. (2006), *The Craft of Intelligence*. Connecticut: Lyons Press.

Ferguson, Harry (2004), *Spy: a Handbook*. London: Bloomsbury.

Ganor, Boaz (2005), *The Counter-Terrorism Puzzle*, New York: Transaction Publishers.

Ganor, Boaz (2012), "Dilemmas and Challenges for the Israel Intelligence Community in Fighting Terrorism", *in* Gilboa, Amos et al. [ed.] *Israel`s Silent Defender, An Inside Look at Sixty Years of Israeli Intelligence*. Jerusalem: Gefen Publishing House.

Gómez, Andrés Montero (2007), "Doctrina de Infiltración para Inteligencia Contraterrorista", *in Athena Paper*, vol. 2 (3), pp. 1-23.

Herman, Michael (2007), Intelligence Power in Peace and War. New Jersey: Princeton University Press.

Johnson, Loch K. (ed.) (2010), *The Oxford Handbook of National Security Intelligence.* New York: Oxford University Press.

Joint Chiefs of Staff (1993), *Joint Tactics, Techniques and Procedures for Antiterrorism* - JP 3-07.2, U.S. Army.

Jones, Ishmael (2010), *The Human Factor, Inside the CIA´s Dysfunctional Intelligence Culture*. New York: Encounter Books.

Kent, Sherman (1951), *Strategic Intelligence For American World Policy*. New Jersey: Princeton University Press.

Lowenthal, Mark M. (2006), *Intelligence: From Secrets To Policy*. Washington: CQ Press.

MacGaffin, John (2005), "Clandestine Human Intelligence – Spies, Counterspies, and Covert Action", in Sims, Jennifer E. et al. (eds.) *Transforming U.S. Intelligence,* pp. 79-95. Washington: Georgetown University Press.

Matos, Hermínio J. de (2011), "O Terrorismo Internacional de Matriz Islamista. A *Intelligence* no Contraterrorismo". Lisboa: Instituto da Defesa Nacional.

Matos, Hermínio J. de (2012a), "E Depois de Bin Laden? Implicações Estratégicas no Fenómeno Terrorista Internacional: Uma Reflexão", *in Politeia*, Ano VIII, 2011, pp. 9-38. Coimbra: ISCPSI.

Matos, Hermínio J. de (2012b) "Contraterrorismo Ofensivo, o "*targeted killing*" na eliminação de alvos terroristas: o caso dos EUA e Israel". Lisboa: ISCPSI (no prelo).

McGarrell, Edmund F. et al. (2007), "Intelligence-Led Policing As a Framework for Responding to Terrorism", *in Journal of Contemporary Criminal Justice*, Volume 23 (2), pp. 142-158.

Pillar, Paul R. (2003), *Terrorism and U.S. Foreign Policy*. Washington: Brookings Institute Press.

Pollard, Neal A. (2009), "On Counterterrorism and Intelligence", *in* Treverton, Gregory *et al*., *National Intelligence Systems*. New York: Cambridge University Press, pp. 117-146.

Ratcliffe, Jerry (2008), *Intelligence-Led Policing*. Oregon: Willan Publishing.

Rego, Helena (2007), "Global Threats Need Global Answers", *in Revista Segurança & Defesa,* n.º 4. Loures: Diário de Bordo.

Rego, Helena (2010), "As Informações na Prevenção do Terrorismo", Comunicação efectuada, em 4 de Maio, na Conferência "Polícia e Informações na Prevenção do Terrorismo". Lisboa: ISCPSI.

Shulsky, Abram N. *et al*. (2002), *Silent Warfare, Understanding the World of Intelligence*. Washington: Potomac Books.

Sims, Jennifer E. et al. (eds.) (2009), *Vaults, Mirrors & Masks. Rediscovering U.S. Counterintelligence*. Washington: Georgetown University Press.

Todd, Paul et al. (2004), *Global Intelligence. The World`s Secret Services Today*. New York: Zed Books.

Torres, José E. Matos (2009), *Terrorismo Islâmico, Gestão dos Riscos para a Segurança Nacional*. Lisboa: EDIUAL.

NOTAS

[1] Indivíduo(s), célula ou organização.

[2] De que são exemplo, entre outros, os EUA e Israel.

[3] Em francês, "*Renseignement Humain*". A HUMINT, e em especial a "clandestine Humint" no contraterrorismo, que é o que aqui nos importa, pode ser definida como a actividade que "includes intelligence obtained from agents planted within the terrorist organizations, deserters and other operatives recruited from the organization`s operational, political or social structures, and operatives who were captured and detained". Cf. Ganor, Boaz (2012), "Dilemmas and Challenges for the Israel Intelligence Community in Fighting Terrorism", *in* Gilboa, Amos *et al*. [ed.] *Israel`s Silent Defender, An Inside Look at Sixty Years of Israeli Intelligence*. Jerusalem: Gefen Publishing House, p. 155.

[4] "Human sources are those individuals who provide information about terrorist organizations and hostile governments. Gathering intelligence from human sources is the fundamental. (…) Lack of good human sources can be a President`s downfall" (Jones, 2010, p. xxiii).

[5] TECHINT – Acrónimo anglo-saxónico que se refere, de um modo geral, à recolha de informações através de meios tecnológicos, compreendendo, *inter alia*, as subdisciplinas: IMINT; MASINT; COMINT; SIGINT, VISINT e OSINT.

[6] OSINT: *Open Source Intelligence*.

[7] Cf. Kent, Sherman (1951), *Strategic Intelligence For American World Policy*. New Jersey: Princeton University Press, p. 3; Herman, Michael (2007), *Intelligence Power in Peace and War*. Cambridge: Cambridge University Press, p. 2. Para uma análise detalhada desta perspective, vide Johnson, Loch K. (ed.) (2010), *The Oxford Handbook of National Security Intelligence.* New York: Oxford University Press, pp. 3-32.

[8] Por exemplo, através do "endurecimento" de medidas legislativas, em especial de índole penal e processual penal (restritivas e punitivas), ou o reforço da segurança em "alvos sensíveis", como infra-estruturas críticas ou simbólicas, aeroportos, fronteiras, grandes eventos, etc.

[9] O *Intelligence-Led Policing* (ILP), ou Modelo de "Policiamento guiado pelas Informações", é uma abordagem holística na prevenção e controlo do fenómeno criminal, através da análise de informações criminais, constituindo-se como instrumento de apoio à decisão que visa a prevenção e redução do crime através de estratégias efectivas, e direccionadas, de policiamento. Cf. Ratcliffe, Jerry (2008), *Intelligence-Led Policing*. Oregon: Willan Publishing, pp. 6-9. Sobre o ILP e a sua aplicação na resposta ao fenómeno terrorista, vide McGarrell, Edmund F. *et al*. (2007), "Intelligence-Led Policing As a Framework for Responding to Terrorism", *in Journal of Contemporary Criminal Justice*, Volume 23 (2), pp. 142-158.

[10] "There is a counterterrorist dimension to counterintelligence (…) Terrorists can and do engage in espionage. Rare is the terrorist attack that is not preceded by surveillance, or «casing», of the target. Terrorists have often be apprehended at the target surveillance stage". Cf. Sims, Jennifer E. *et al.* (eds.) (2009), *Vaults, Mirrors & Masks. Rediscovering U.S. Counterintelligence*. Washington: Georgetown University Press, p. 263.

[11] Grosso modo, e numa perspectiva classificatória quanto às fontes de informação, existem três tipos de *Intelligence*: 1) "*Black Intelligence*", se proveniente de fontes "cobertas" ou secretas; 2) "*White Intelligence*", obtidas através de "fontes abertas"; 3) "*Grey Intelligence*", uma tipologia intermédia que designa "information which is not published or widely diffused, but to which access can be gained, provided that one knows it exists and has adequate channels of information. (…) It is information which is difficult to find or is protected by very low-level restrictions". Cf. Ferguson, Harry (2004), *Spy: a Handbook*. London: Bloomsbury, pp. 72-73.

[12] Ao processo de direcção e controlo da "fonte" por parte do "Case Officer" (Oficial de Informações ou "handler", que pode não ser o "recrutador"), a terminologia anglo-saxónica designa por "handling" ou "agent running". Sobre este assunto, vide Shulsky *et al*. (2002); Dulles (2006) e Ferguson (2004).

[13] "A legend is the support structure for a cover. Thus some covers have almost no legends at all. Some deep covers have very detailed legends wich need a considerable staff to keep them up to date. In the most extreme cases (sleepers), the legend is something you live and constantly create. It is indistinguishable from your real life". Cf. Ferguson, Idem, pp. 60-61.

[14] Geralmente efectuada por uma equipa de analistas especializados, sedeada na "central" dos serviços, designada por "Profiling Team".

[15] Operado em torno de uma matriz de "motivações" designada por MICE: "Money", "Interest", "Constraint" e "Ego". Cf. Desmaretz, Gérard (2007), *Le Renseignement Humain*. Paris : Chiron Éditeur, p.29. Ou "Money" , "Ideology", "Compromission" e "Ego"; Cf. Denécé, Éric (2008), *Renseignement et Contre-Espionnage. Actions Clandestines, Technologies, Services Secrets*. Paris : Hachette, p.68. São possíveis outras "catalogações" que enquadram: amor, sexo, vingança, vaidade, culpa, etc. O essencial é identificar a existência dessa motivação, ou vulnerabilidade, consoante o ponto de vista de análise, e explorá-la de forma adequada.

[16] No caso de um grupo ou organização terrorista, a abordagem integrada está fora de questão uma vez que estas são estruturas que se movem em contextos muito fechados, e de elevada segurança, pelo que se torna impossível a colocação de outras "personagens" credíveis em cena.