

A Produção de Inteligência Contraterrorista: o papel da *Human Intelligence*

Diogo Filipe Escudeiro Lopes

Orientador: Prof. Doutor Pedro João Borges Graça

Dissertação para obtenção de grau de Mestre
em Estratégia

Lisboa
2020

WWW.ISCSP.U LISBOA.PT

A Produção de Inteligência Contraterrorista: o papel da *Human Intelligence*

Diogo Filipe Escudeiro Lopes

Orientador: Prof. Doutor Pedro João Borges Graça

Dissertação para obtenção de grau de Mestre
em Estratégia

Júri

Presidente:

- Doutor Heitor Alberto Coelho Barras Romana, Professor Catedrático do Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa;

Vogais:

- Doutor António Manuel Fernandes da Silva Ribeiro, Professor Catedrático Convidado do Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa;

- Doutor Pedro João Borges Graça, Professor Associado do Instituto Superior de Ciências Sociais e Políticas da Universidade de Lisboa, na qualidade de Orientador.

Lisboa
2020

AGRADECIMENTOS

Quero expressar o meu primeiro agradecimento ao ISCSP, pelas portas que me abriu em múltiplos níveis, desde o primeiro momento em que iniciei este mestrado até ao momento em que escrevo, de forma singela, estas palavras. A forma como me fez olhar para a vida académica, profissional e também pessoal de diferente modo, abrindo conhecimentos, horizontes e até mesmo sonhos. Agradeço ao ISCSP enquanto instituição, mas também, de forma não menos importante, a todos os professores que direta ou indiretamente me foram direcionando e alimentando a minha vontade de conhecer. Agradeço, também, a todos os funcionários não docentes que desobstruíram e clarificaram caminhos, que por vezes aparentaram ser intransponíveis.

Quero manifestar o meu profundo agradecimento ao Professor Doutor Pedro João Borges Graça por toda a orientação que me foi concedida. Agradeço ao Professor a dedicação, a disponibilidade, a minúcia e, acima de tudo, o interesse que demonstrou no acompanhamento do meu trabalho, criticando, esclarecendo e “alimentando” a minha investigação com pormenores que se revelaram basilares.

Agradeço à minha “casa”, a Polícia de Segurança Pública, que me apoiou e tem apoiado sistematicamente nestes desvios científicos, permitindo toda a articulação entre os momentos de estudo e os de atividade laboral. Por reconhecer a pertinência das matérias que tenho trabalhado e das competências que tenho adquirido, no plano académico, valorizando-as e conciliando-as com as tarefas que me passaram a ser incumbidas diariamente. Este reconhecimento motiva-me, tanto profissionalmente como pessoalmente.

Por fim, e de modo não menos importante, justamente pelo contrário, agradeço à minha mulher e aos meus pais, por todo o apoio incondicional, por toda a compreensão em momentos facilmente incompreensíveis, por todo o altruísmo genuinamente desinteressado. Agradeço a força que me deram de forma permanente, auxiliando-me de múltiplas formas, sempre de modo abnegado.

A todos os que me fizeram olhar em frente e caminhar, muito obrigado.

RESUMO

A sequência de atentados terroristas, no dia 11 de setembro de 2001, nos Estados Unidos da América, despertaram no mundo ocidental a consciência da vulnerabilidade das populações face à violência terrorista. Este dia, seguido de outros similares, noutras partes do globo, determinaram a urgência da produção de inteligência de natureza contraterrorista, que até a este momento tinha sido colocada em segundo plano, face a outras questões tidas como prioritárias no mundo da inteligência. Este trabalho debruça-se sobre esta temática, a produção de inteligência contraterrorista, procurando, de um modo mais concreto, circunscrever a investigação à metodologia de pesquisa HUMINT. Limita-se, também, geograficamente, ao eixo anglo-americano e, cronologicamente, às últimas duas décadas, a era pós 11 de setembro. Numa época em que as informações provenientes de fontes abertas proliferaram e os meios de recolha eletrónica deram um salto qualitativo de relevo, procura-se compreender como se atua hodiernamente, no plano das informações obtidas pela via humana. A investigação visa conhecer como se aplica hoje a HUMINT no contraterrorismo e qual o seu papel na panóplia das outras metodologias de pesquisa.

Palavras-Chave: Inteligência; *Human Intelligence*; Terrorismo; Contraterrorismo;

ABSTRACT

The sequence of attacks in the United States of America on the 11th of September 2001 awakened the western world to the vulnerability of populations to terrorism. This day, along with similar incidents that ensued in other parts of the globe, determined the urgency for counterterrorism intelligence, which until then had remained in the background, in comparison to other issues deemed a priority in the world of intelligence. This thesis focuses on the production of counterterrorism intelligence, with an emphasis on the HUMINT collection methodology applied after the 9/11 attacks in the Anglo-American axis. At a time in which open-source information proliferates and technology used to assist in data collection is greater than ever, we seek to understand how nowadays information is obtained through human sources. Therefore, this investigation aims to understand the contemporary role of HUMINT among the other counterterrorism information collection methodologies.

Key words: *Intelligence; Human Intelligence; Terrorism; Counterterrorism;*

ÍNDICE

| | |
|--|------------|
| AGRADECIMENTOS | I |
| RESUMO | III |
| ABSTRACT | V |
| ABREVIATURAS | IX |
| INTRODUÇÃO: O OBJETO DE ESTUDO | 1 |
| Enquadramento | 1 |
| Objetivos | 2 |
| METODOLOGIA | 4 |
| 1. A PERSPETIVA DA ESTRATÉGIA | 7 |
| 1.1. O Conceito de Estratégia | 7 |
| 1.2. A Fase da Análise no Processo Estratégico | 10 |
| 1.3. A Função da Inteligência | 13 |
| 1.3.1. A Pluralidade Conceptual da Inteligência | 13 |
| 1.3.2. O Ciclo de Produção de Inteligência | 16 |
| 1.3.2.1. Requisitos | 17 |
| 1.3.2.2. Pesquisa | 18 |
| 1.3.2.3. Processamento e Exploração | 20 |
| 1.3.2.4. Análise e Produção | 22 |
| 1.3.2.5. Disseminação e Consumo | 23 |
| 1.3.2.6. <i>Feedback</i> | 24 |
| 2. O FENÓMONO DO TERRORISMO | 25 |
| 2.1. O Conceito de Terrorismo | 25 |
| 2.2. O Panorama Atual do Terrorismo | 28 |
| 2.3. A Abordagem do Contraterrorismo | 35 |
| 3. A HUMAN INTELLIGENCE NO CONTRATERRORISMO ANGLO-AMERICANO | 39 |

| | |
|--|-----------|
| 3.1. Metodologia da <i>Human Intelligence</i> | 39 |
| 3.2. O Panorama Estrutural dos Serviços de Inteligência no Eixo Anglo-americano | 42 |
| 3.2.1. Estrutura da Inteligência nos EUA | 42 |
| 3.2.2. Estrutura da Inteligência no Reino Unido | 45 |
| 3.3. Práticas Norte-americanas | 47 |
| 3.3.1. <i>Army Intelligence</i> | 47 |
| 3.3.2. <i>Department of Defense</i> (DoD) | 54 |
| 3.3.3. <i>Central Intelligence Agency</i> (CIA) | 59 |
| 3.4. Práticas britânicas | 61 |
| 3.4.1. <i>British Army</i> | 61 |
| 3.4.2. <i>Security Service</i> (MI5) | 64 |
| | |
| CONCLUSÕES | 71 |
| REFERÊNCIA BIBLIOGRÁFICAS | 77 |
| | |
| Livros e Artigos | 77 |
| Documentos | 84 |
| Websites | 86 |
| | |
| ANEXO I | 91 |
| | |
| 1. Evolução do Terrorismo ao Nível Mundial | 93 |
| 2. Evolução do Terrosimo por Região do Mundo (entre 2001 e 2018) | 94 |
| 3. Evolução do Terrorismo no Reino Unido | 95 |
| 4. Evolução do Terrorismo nos Estados Unidos da Améria | 96 |
| | |
| ANEXO II | 97 |

ABREVIATURAS

CIA – *Central Intelligence Agency*

COMINT – *Communications Intelligence*

DI – *Defense Intelligence*

DIA – *Defense Intelligence Agency*

DoD – *Department of Defense*

ELINT - *Electronic Intelligence*

EU – *União Europeia*

EUA - *Estados Unidos das América*

FBI – *Federal Bureau of Investigation*

FISINT - *Foreign Instrumentation Signals Intelligence*

FSSD – *Forças e Serviços de Segurança e Defesa*

GCHQ - *Government Communications Headquarters*

GEOINT - *Geospatial Intelligence*

GTD – *Global Terrorism Database*

HUMINT – *Human Intelligence*

IC – *Intelligence Community*

IMINT - *Imagery Intelligence*

IRA – *Irish Republican Army*

IRN - *Department of State Bureau of Intelligence and Research*

ISIL – *Islamic Stat of Iraq and the Levant*

ISTAR - *Intelligence, Surveillance, Target Acquisition and Reconnaissance*

JIO - *Joint Intelligence Organization*

MASINT - *Measurement and Signature Intelligence*

MI5 – *Security Service*

NSA – *National Security Agency*

NSS - *National Security Secretariat*

ONG – *Organização Não Governamental*

ONU – *Organização das Nações Unidas*

OSCT - *Office for Security and Counter-Terrorism*

OSIF – *Open Source Information*

OSINT – *Open Source Intelligence*

OTAN – *Organização do Tratado Atlântico Norte*

PESTEL - *Political, Economic, Social, Technological, Environmental and Legal*

PHOTINT - *Photo Intelligence*

RU – *Reino Unido*

SIGINT – *Signals Intelligence*

SIS – *Secret Intelligence Service*

SWOT - *Strengths, Weaknesses, Opportunities and Threats*

TECHINT - *Technical Intelligence*

TELINT - *Telemetry Intelligence*

USCG - *Coast Guard*

INTRODUÇÃO: O OBJETO DE ESTUDO

ENQUADRAMENTO

O terrorismo é hoje um dos fenômenos políticos mais preponderantes no espectro global pelo seu impacto no plano securitário, refletindo-se no medo causado às pessoas no que diz respeito à sua vida, integridade física ou mesmo danos patrimoniais particulares. Apesar da gênese do método subversivo ser a aquisição do poder político, e que não deixa de ser “um dos processos contemporâneos mais eficientes neste âmbito” (Lara, 2015, p. 448), a repercussão dos atos perpetuados reflete-se também no condicionamento do regular curso individual de vida dos cidadãos.

Apesar do impacto do terrorismo ser mais preponderante nas regiões do Médio Oriente, África e sul da Ásia, sendo que só os países Afeganistão, Iraque, Nigéria, Somália e Síria contemplam 74% das mortes resultantes do terrorismo em todo o globo (Institute for Economics & Peace, 2019, p. 12), este continua a ser preocupante para o mundo ocidental, resultando permanentemente em ações estaduais políticas e legislativas de países, individualmente, e outras de cariz supranacional, envolvendo organizações como a União Europeia (EU), a Organização do Tratado Atlântico Norte (OTAN) ou a Organização das Nações Unidas (ONU).

Pelo quarto ano consecutivo, o número de mortes geradas por este fenómeno tem decrescido, olhando à globalidade (Institute for Economics & Peace, 2019, p. 12), sendo que, no entanto, a realidade ocidental não é a mesma. Em 2018, na Europa Ocidental e na América do Norte, 106 pessoas morreram em consequência de atos terroristas, sendo este valor superior à média dos anos do presente milénio (84 mortes)¹. Em termos de incidentes, a realidade é similar, crescendo de 210 atentados por ano (em média) para 302 em 2018 (START, 2019). O mundo ocidental não está hoje mais imune ao terrorismo.

No combate ao fenómeno terrorista muitos têm sido os instrumentos de cariz defensivo e ofensivo aplicados na mitigação deste, sendo que a inteligência, essencialmente no plano

¹ Excluindo o fatídico e anómalo ano de 2001, com a sequência de atentados ocorridos nos EUA, atingindo os três milhares de mortes.

ofensivo, tem sido a peça base na disrupção de células terroristas e detecção precoce de indivíduos solitários com afinidade parcialmente formal a organizações terroristas. Desde 2001 que a própria inteligência se tem ocupado com maior predominância no fenómeno terrorista (com especial ênfase no terrorismo de matriz islâmica), sendo este o seu principal foco de trabalho, considerando “o impacto que o terrorismo pode exercer sobre a macroestrutura política dos Estados e na estabilidade global das sociedades” (Romana, 2004, p. 264)

Com vista à produção de inteligência contraterrorista, no âmbito do próprio ciclo de produção de inteligência, diversas metodologias têm sido adotadas na pesquisa de informações, conducentes a uma eficaz produção de inteligência capacitadora da tomada de decisão estratégica e operacional. Uma delas, a *Human Intelligence* (HUMINT), designada tradicionalmente por espionagem, tem se revelado crucial na obtenção de elementos informativos, sendo que, segundo Mayer (2016, p. 6), é um dos componentes chave da disrupção do fenómeno terrorista passará pelo investimento significativo nesta forma de pesquisa, nomeadamente no incremento desta valência nas forças de segurança locais.

Tomando como exemplo o fracasso dos serviços de inteligência norte americanos na prospeção do conjunto de atentados que ocorreram em 2001 nos Estados Unidos da América (EUA), perpetrados pela *Al-Qaida*, associado à quase total ausência de fontes humanas dentro daquela organização, segundo Aid (2009, p. 47), interessa conhecer a preponderância dada hoje à HUMINT e quais os métodos aplicados, em concreto, pelos serviços de inteligência nesta esfera. Conjugando a consciência (pós 11 de Setembro) da necessidade do incremento de ações clandestinas e encobertas e respetiva recolha de informações mais próxima dos alvos (Aid, 2009, p. 66) com o contemporâneo acréscimo de impacto terrorista no ocidente, julgou-se pertinente a investigação, associada à produção da presente dissertação.

OBJETIVOS

O tema central da investigação foca-se na temática da inteligência, na vertente do contra-terrorismo, sendo o problema de investigação o estado da arte da HUMINT no eixo anglo-americano, conduzindo à questão central:

- *Qual é, hodiernamente, a metodologia de HUMINT na tarefa de produção de inteligência contraterrorista?*

Tendo como base geográfica de trabalho o eixo anglo-americano, procurou-se dar resposta à questão colocada circunscrevendo-a, cumulativamente, a um escopo investigatório muito específico e de cariz prático. Visou-se, portanto, estudar somente a metodologia de pesquisa de inteligência HUMINT no vasto espectro do ciclo de produção de inteligência, limitando-a exclusivamente ao foro do contraterrorismo. Não foi ambição deste trabalho pormenorizar as restantes envolvências inerentes à produção de inteligência, nem a outros focos de intervenção desta.

Salienta-se que, em matéria cronológica, serão consideradas fontes pós ano 2001, especialmente aquando da especificação dos métodos aplicados atualmente pelas forças e serviços de segurança e defesa (FSSD) dos respetivos países. O motivo dessa data ser assumida como ponto cronológico inicial, prende-se com o facto de ser o ano mais marcante para o mundo ocidental em matéria de terrorismo, considerando a sequência de atentados ocorridos a 11 de setembro nos EUA. Em suma, foi alvo desta investigação as práticas de HUMINT no contraterrorismo do Reino Unido (RU) e dos EUA, a partir de 11 de setembro de 2001.

Com maior especificidade, e intimamente correlacionada com a questão central, procurar-se-á também responder às seguintes questões derivadas:

- *Qual é o papel da HUMINT na tarefa de produção de inteligência contraterrorista?*
- *Qual o relevo dado à HUMINT por estes países, em contraposição com outras formas de pesquisa?*

Atendendo à questão central e às questões derivadas, investigou-se o estado da arte da HUMINT nestas nações, compreendendo o *modus operandi* no que diz respeito à aplicação de fontes humanas no combate ao fenómeno do terrorismo.

A maior limitação na consumação da investigação em apreço foi o facto de a temática estar, em grande medida, revestida de confidencialidade. Foi assim, naturalmente, dificultada a recolha de dados ilustrativos da aplicação dada pelas FSSD a este método de pesquisa de informações, no plano contraterrorista, nos dias de hoje. Procurou-se, no entanto, cruzar informações bibliográficas diversificadas, capazes de caracterizar o estado atual da HUMINT no contraterrorismo.

METODOLOGIA

No âmbito desta investigação, visou-se abordá-la de um prisma qualitativo, não a matematizando, em matéria de pesquisa ou nas conclusões obtidas. Atendendo à pergunta de partida, almejou-se efetuar um percurso sequencial teórico, sendo intenção operacionalizar os conceitos chave de estratégia e terrorismo. Primeiramente, no campo da estratégia, procurou-se conhecer o conceito em termos genéricos, podendo, posteriormente, avançar para a perceção do processo estratégico com especial ênfase na fase primária deste, a análise. Aliada a esta fase, abordou-se ainda, num plano teórico, o processo de produção de inteligência, aprofundando de algum modo a fase da pesquisa de informações neste processo, afinando a revisão teórica, de acordo com a temática proposta.

Numa segunda fase, aquando da exploração do termo terrorismo, compreendeu-se a problemática deste, no campo da sua definição conceptual, aliado a outros conceitos correlacionados, tais como o de *ordem*, de *subversão* e de *contraterrorismo*. Elaborou-se, em complemento à revisão teórica, uma abordagem sistemática ao panorama atual do fenómeno do terrorismo e atentados associados nos locais geográficos abordados nesta investigação, EUA e RU. Esta abordagem qualitativa da estatística procurou estabelecer uma ponte entre a revisão conceptual enformadora do trabalho e o propósito crucial deste, designadamente, a compreensão dos métodos utilizados atualmente na produção de informações contraterroristas no campo da HUMINT.

Nesta última fase, tendo como enfoque o eixo anglo-americano, foi intenção compreender o *modus operandi* das FSSD na utilização da HUMINT no contraterrorismo, constatando eventuais práticas de infiltração e/ou penetração no seio das organizações terroristas. Visou-se, cumulativamente, compreender a interligação da HUMINT com outros métodos de

pesquisa, assim como os obstáculos apresentados atualmente no contraterrorismo desenvolvido por estes dois países, nomeadamente perante a utilização da forma de pesquisa abordada.

De modo a responder à pergunta de partida, para além da exploração de fontes bibliográficas ambiciosamente diversificada, promoveu-se, portanto, conforme referido anteriormente, uma recolha de dados estatísticos, relativos ao fenómeno do terrorismo. Esta recolha cingiu-se somente ao espaço geográfico anglo-americano, sendo o lapso temporal relativamente reduzido, limitando-a às últimas duas décadas, nomeadamente a partir de 11 de setembro de 2001, pelos motivos anteriormente expostos.

1. A PERSPETIVA DA ESTRATÉGIA

1.1. O CONCEITO DE ESTRATÉGIA

A estratégia, segundo André Beaufre (2004, p. 35), numa perspectiva mais clássica, é a “arte de utilizar a força para a concretização dos objetivos da política”. Num plano militar, mas cumulativamente político, Duarte (2013, p. 63) afirma que a “estratégia brotou da necessidade dos atores adquirirem aptidões para controlar e regular a manipulação e gestão do aniquilamento, feito através da luta e do combate, com vista a atingir os fins desejados, sobrepujando as resistências que os adversários lhes ofereciam”.

Este é um conceito que poderá ser interpretado por duas vias, enquanto ciência e enquanto arte. António Silva Ribeiro (2010, p. 22) esclarece que esta é a “ciência e a arte de edificar, dispor e empregar meios de coação num dado meio e tempo, para se materializarem objetivos fixados pela política, superando problemas e explorando eventualidades num dado ambiente de desacordo”. Também, à semelhança do conceito operacional anteriormente utilizado, é a “ciência e arte de desenvolver e utilizar as forças morais e materiais de um ator político ou coligação, a fim de se atingirem objetivos políticos que suscitem, ou podem suscitar, a hostilidade de uma outra vontade política” (Couto, 1988, p. 207).

Enquanto arte, “a estratégia permite, independentemente de qualquer técnica, dominar os problemas que só por si são colocados por qualquer duelo, para permitir justamente utilizar as técnicas com o máximo de eficácia” (Beaufre, 2004, p. 36). Esta é a “combinação dos fatores de decisão usando, para cada um deles, a parte subjetiva e parte objetiva dos fatores que compõem o cálculo estratégico (denominadas de provas da estratégia), seguindo os critérios de *adequabilidade, exequibilidade e aceitabilidade*” (Ribeiro, 2010, p. 23). Enquanto ciência, a estratégia “compõe-se de um objeto preciso, suscetível de investigação e análise, recorrendo a instrumentos teóricos e práticos independentes, ciclicamente transformados pela atividade intelectual”, explicando “convenientemente os fenómenos estratégicos (factos e acontecimentos) quanto à sua essência, casualidade e efeitos, socorrendo-se de ferramentas práticas (técnicas) próprias ou de outras ciências sociais” (Ribeiro, 2010, p. 23).

Escrutinando a dicotomia ciência e arte, Ribeiro (2010, p. 31) acrescenta, ainda, que “ser mestre na arte da estratégia não é o mesmo que ter o chamado gênio estratégico. Este, revela uma habilidade transcendente para perceber o centro de gravidade do contrário e para imaginar a articulação dos fatores de decisão, segundo a modalidade de ação mais eficaz e eficiente, para provocar o desequilíbrio estratégico.”

No que diz respeito ao planejamento estratégico, Sun Tzu (2009, p. 12) afirma que este é crucial na definição do curso e do resultado de um dado objetivo, nomeadamente no sucesso. Afirma que “O general que vence a batalha faz muitos cálculos antes de a travar. O general que perde a batalha faz poucos cálculos antecipadamente. Assim, muitos cálculos levam à vitória e poucos à derrota. Quem não fizer cálculo algum terá ainda menos possibilidades de vencer. É considerando este ponto que posso antever quem irá ganhar ou perder”.

Associado ao conceito de estratégia, dever-se-á conhecer o de guerra. Esta, enquanto “duelo em grande escala”, deverá ser definida como “um ato de violência com que se pretende obrigar o nosso oponente a obedecer à nossa vontade (...) por meio de força física, compelir o outro a submeter-se à sua vontade” (Clausewitz, 1997, p. 29). Correlacionando os dois conceitos, Duarte (2013, p. 35) esclarece que “a guerra nasce no ato de confrontar e no enredamento engendrado pelo movimento bélico, a estratégia desponta da sistematização do pensamento sobre esse ato de confrontação e sobre a lógica do enredamento bélico”. Afirma ainda que a “estratégia é uma linguagem de análise, uma hermenêutica” (Duarte, 2013, p. 35). No âmbito da tradicional associação da estratégia com a guerra, esta última nasce da primeira “como réplica à complexidade da «relação paradoxal» criada pelo cada vez mais enredado e longamente tecido jogo político-bélico da modernidade.” (Duarte, 2013, p. 51)

Na sequência dos conceitos de estratégia e de guerra, dever-se-á abordar o de segurança, já que a estratégia, no plano estadual, é instrumentalizada para a conservação da sociedade política, visando essencialmente a garantia da segurança nacional, procurando a “preservação da identidade e a sobrevivência de uma unidade política, ou, dito de outra forma, a independência e a integridade nacional” (Ribeiro, 2010, p. 48). Conceptualmente, a segurança assume-se como um “conceito poliédrico, podendo diferenciar-se ou enroupar mais que um quadro físico-intelectual conforme o fim e o domínio em que se desenvolve. A poliedricidade da segurança provoca uma análise que, por ser densa, pode ser confusa e trazer (...) uma

amalgama de considerações que, necessariamente, imbricam com o conceito de *segurança pública*, sendo que este ancora em um conceito mais amplo, o de *segurança interna*” (Valente, 2014, p. 291).

A segurança pode então ser vista como um “estado ou condição que se estabelece num determinado ambiente, através da utilização de medidas apropriadas, com vista à sua preservação e à condução de atividades, no seu interior ou em seu proveito, sem ruturas. Poderá ser analisada enquanto *safety* (medidas conducentes a afastar o perigo) e *security* (medidas destinadas a limitar as perdas, manter a ordem e a socorrer), sendo que ambas as terminologias contribuem para estabelecer um clima de libertação do perigo” (Alves, 2010, p. 32).

Este conceito poderá ainda assumir duas modalidades, a *interna* e a *externa* (independentemente da natural, e cada vez mais comum, ausência de segregação entre conceitos, pela sua interdependência no plano operacional). A *interna* pauta-se pela sua imprescindibilidade na consolidação da democracia e no exercício dos direitos e liberdades dos cidadãos, criando condições de segurança, ordem e tranquilidade públicas necessárias e essenciais ao desenvolvimento económico, à promoção e consolidação da qualidade de vida dos cidadãos (Fernandes L. F., 2014, p. 37). A *externa*, “que se aquela que se arrega no conceito constitucional de defesa-segurança-nacional, deve ser entendida (...) como a segurança que está direcionada em exclusivo para a segurança do país contra ameaças e agressões externas” (Valente, 2014, p. 299).

Ainda sobre a segurança externa, também denominada de defesa nacional, a Constituição da República Portuguesa (1976) declara que esta visa “garantir, no respeito da ordem constitucional, das instituições democráticas e das convenções internacionais, a independência nacional, a integridade do território e a liberdade e a segurança das populações contra qualquer agressão ou ameaça externas.” A defesa nacional é também o “conjunto de atos que permitem ao Estado proteger-se de uma ameaça pontual, latente ou concretizada, que afete os interesses nacionais”, surgindo, assim, como “uma atividade que visa garantir a segurança nacional” (Ribeiro, 2010, p. 55). Esta deve ser entendida como a “produção, organização e emprego dos meios militares” (Loureiro dos Santos, 2001, p. 30).

Enquanto fusão conceptual das duas, segurança interna e externa, a segurança nacional, poderá ser definida como “um conjunto de interesses, que podem ir desde a garantia de acesso a matérias primas essenciais, até à proteção de investimentos e de cidadãos nacionais no estrangeiro, desde cinturas de segurança a zonas de influência ou neutralizadas, desde o controlo do nível de capacidade militar de adversários potenciais e vizinhos, até à uniformidade dos regimes e sistemas políticos” (Couto, 1988, p. 71)

No plano científico, a estratégia, desenvolvida enquanto estudos estratégicos, “tem sido tradicionalmente confrontada com o problema da definição e delimitação do seu objeto, tendo desde logo esclarecer a sua interligação com os Estudos de Segurança, os quais, por causa da sua *condição supradisciplinar*, vão desde as questões abrangentes da segurança nacional às mais específicas da *segurança da informação* ou da *segurança económica*” (Graça, 2014, p. 74). No plano metodológico, “no ponto de vista do objeto de estudo a definir e delimitar, não basta ao investigador analisar somente e estritamente a relação entre Estratégia e Política, é necessário refletir sobre a perspetiva abrangente da área dos Estudos Estratégicos e a correlativa noção da sua complexidade interdisciplinar, existindo uma pluralidade de interações disciplinares que traduzem epistemologicamente a realidade, não só no âmbito político, mas também no económico, social e cultural” (Graça, 2014, p. 77). Os estudos estratégicos não deverão cingir-se à área dos estudos militares, sendo essa uma perspetiva redutora, “resultante de uma visão clássica da Estratégia, historicamente veiculada por autores militares” (Graça, 2014, p. 78).²

1.2. A FASE DA ANÁLISE NO PROCESSO ESTRATÉGICO

“O processo estratégico tem uma estrutura lógica ou esquema dialético, designado por modalidade de ação estratégica ou manobra estratégica (...) são previstas as reações do competidor a cada uma das ações próprias consideradas, de natureza política, económica,

² Graça (2014, p. 79) apresenta uma hipótese de reformulação, no que diz respeito à conexão dos “estudos de área”, colocando os estudos estratégicos inseridos nas relações internacionais/estudos internacionais e, por sua vez, dentro dos primeiros, os “estudos de área” específicos, nomeadamente os estudos de competição, estudos de conflito, estudos de defesa, estudos de inteligência, estudos militares, estudos de paz, estudos de terrorismo, estudos de guerra, entre outros. Não adota o modelo Baylis, Wirtz & Gray, onde a ciência política abarca as relações internacionais que, por sua vez, abarca os estudos de segurança, contemplando, estes últimos, os estudos estratégicos, e por fim, mais especificamente, os estudos militares. Apresenta ainda uma outra hipótese estrutural, onde os Estudos Estratégicos são centrais e os outros estudos de áreas (estudos de inteligência, estudos de paz, estudos militares, estudos de terrorismo, entre outros) daqueles derivam, assumindo os primeiros uma posição central para com os segundos.

psicossocial e militar, procurando evitar ou ultrapassar cada uma delas (...)Articulam-se com habilidade os fatores de decisão, segundo os princípios e as regras estratégicas de aplicação, de forma a alcançar a vantagem estratégica, tendo em vista afetar o centro de gravidade do contrário” (Ribeiro, 2010, p. 99).

O processo estratégico, enquanto caminho percorrido com *terminus* na consumação dos objetivos fixados (ambiciosamente), poderá ser caracterizado de várias formas e com várias fases. Ribeiro (2017, p. 27), no modelo aplicado à Marinha Portuguesa, inspirado no modelo *Palladium Execution Premium Process*³, contempla três fases primordiais: a da *formulação*, a da *operacionalização* e a do *controle*. A primeira almeja, inicialmente, analisar o ambiente e formular a estratégia propriamente dita. A segunda visa traduzir a estratégia (que ações serão executadas e por quem), alinhando a organização e planejando as atividades. A terceira fase procura monitorizar/aprender e testar/adaptar, assegurando que o desempenho real é equivalente aos padrões estabelecidos. Correia (2015, p. 67) e Wheelen & Hunger (1989, p. 10), por outro lado, defendem um modelo de quatro díspares fases, acrescentando às três anteriormente apresentadas, a fase do pensamento estratégico (ou análise estratégica), ou seja, não consideram a análise uma subfase da *formulação*, mas sim uma prévia etapa independente.

A fase da análise do ambiente, enquanto início do processo estratégico, poder-se-á considerar a fase da produção de inteligência estratégica⁴ (especialmente no respeitante à vertente externa, como irá ser abordado seguidamente). Com vista à clarificação do estrategista e sustentação na sua tomada de decisão no curso do processo estratégico, dever-se-á analisar o panorama que poderá influenciar o sucesso de determinada organização. Deverá esta fase incluir uma avaliação abrangente dos seus próprios recursos e desempenho destes em comparação com os seus concorrentes, bem como o posicionamento da organização em relação às tendências do setor onde esta se insere (Kaplan & Norton, 2008, p. 47).

Neste âmbito, Cardoso (2004, p. 146) afirma que “onde o governante tem que ser hábil,

³ Evolução da *Balanced Scorecard* de Robert Kaplan e David Norton (2008, pp. 8-18), onde o ciclo se inicia com o desenvolvimento da estratégia, seguindo-se a tradução da estratégia, o alinhamento da organização, o planeamento das operações, a execução, a monitorização e aprendizagem e, por fim, o teste e a adaptação.

⁴ Naturalmente, dada a temática da investigação realizada, o enfoque estará nesta fase, no que diz respeito à clarificação do processo estratégico.

dominante e objetivo é nas análises, previsões e estudos prospetivos, para reduzir ao mínimo a surpresa e impreparação do aparelho de Estado para fazer face aos acontecimentos”. O autor atribui significativa preponderância à prévia análise, no curso da aplicação da estratégia, considerando que as “organizações dever-se-ão manter informadas e esclarecidas, elaborando análises prospetivas, procurando isolar, com oportunidade, as vantagens e inconvenientes, a curto, médio e longo prazo, para que a organizações estejam preparadas no prisma externo” (Cardoso, 2004, p. 162). No entanto, não só a nível externo se deverá promover a prévia análise, anterior à marcha do processo estratégico, devendo ser também efetuada uma introspetiva. Procurar-se-á detetar as oportunidades e ameaças externas e assimilar as potencialidades e vulnerabilidades internas (Ribeiro, 2017, p. 31).

No plano interno da organização, poderá ser utilizado o método SWOT, sendo apuradas a potencialidades, as vulnerabilidades, as oportunidades e as ameaças⁵ (Kaplan & Norton, 2008, p. 10). Procurar-se-á com este método, ou outros, conhecer a conjuntura interna da organização e o seu posicionamento num plano externo, não limitando, assim, a perceção que a organização tem de si mesma. A perceção externa e interna da organização (desejavelmente plena) conduzirá ao sucesso estratégico. A propósito, Sun Tzu (2009, p. 24) observa: “Aquele que conhece o inimigo e se conhece a si mesmo sairá vitorioso de cem batalhas; aquele que se conhece a si mesmo mas não conhece o inimigo por vitória conquistada conhecerá uma derrota; aquele que não se conhece a si nem ao inimigo será derrotado em todas as batalhas”

Como instrumento de análise externa do ambiente, poderá ser utilizada a análise PESTEL, onde serão avaliados os aspetos políticos, económicos, sociais, tecnológicos, ambientais e legais⁶. Esta técnica “possibilitará antecipar as tendências futuras (...) facilitando, dessa forma, a determinação dos fatores externos gerais que irão influenciar determinada organização nos próximos anos” (Ribeiro, 2017, p. 32). Os fatores externos podem “constituir ameaças, isto é, condições ambientais desfavoráveis, capazes de afetar negativamente a organização, caso não sejam contidos ou eliminados”, mas, no entanto, também podem “traduzir oportunidades, isto é, condições ambientais favoráveis, suscetíveis de trazer uma vantagem competitiva” à organização, se esta for oportuna no seu aproveitamento (Ribeiro, 2017, p. 32).

5 Em inglês, e em correspondência com a sigla SWOT, *Strengths, Weaknesses, Opportunities e Threats*.

6 Em inglês, e em correspondência com a sigla PESTEL, *Political, Economic, Social, Technological, Environmental e Legal*.

Uma vez concretizada a análise interna e externa, será viável prosseguir para a prospeção estratégica. Assim que uma organização tiver recolhido os dados necessários à compreensão da situação ambiente, deverá analisar as tendências atuais, compreendendo se elas continuarão no futuro. Somente após os passos mencionados, deverão ser feitas assunções para o planeamento estratégico e posterior tomada de decisão (Wheelen & Hunger, 1989, p. 109). “Qualquer estratégia só é aplicável – seja ela boa ou má – depois de haver um processo de decisão. O processo de decisão depende, entre outros fatores, da Informação” (Jesus, 2015, p. 21).

1.3. A FUNÇÃO DA INTELIGÊNCIA

1.3.1. A PLURALIDADE CONCEPTUAL DA INTELIGÊNCIA

Segundo Lowenthal (2003, p. 2), a inteligência é a informação recolhida, selecionada e refinada que vai de encontro às necessidades dos decisores políticos. Esta deve ser coadjuvante à política e não um formulador de políticas por si só, já que as prioridades da inteligência devem refletir as prioridades políticas (Lowenthal, 2003, p. 43). A inteligência deverá ser, exclusivamente, um instrumento da política. O seu objetivo deverá ser a redução do grau de incerteza destes decisores ao mínimo possível (Wheaton & Beerbower, 2006, p. 329).

A inteligência é mais do que informação. A “informação, por si só, não dá a ideia da forma como os atores irão agir, quais serão os modelos de atuação, os sentidos a atingir, bem como a oportunidade de aplicação do seu esforço (...) é somente um conjunto de dados colocados num contexto, relacionados com o espaço, o tempo e o cenário da ação” (Bispo, 2004, p. 78). A inteligência, por sua vez, é a “compreensão da informação relacionada, organizada e contextualizada” (Bispo, 2004, p. 78). A inteligência é a “integração e interpretação das informações, num determinado contexto e para um determinado fim, que permitem a geração de conhecimento materializado em inteligência e esta, uma vez difundida aos utilizadores finais, tem potencial para gerar novo conhecimento” (Fernandes L. F., 2014, p. 80). Poder-se-á afirmar, então, que a inteligência é o conjunto de informações recolhidas, num estado evolutivo díspar da informação (enquanto elemento primário), onde todo um processo congregou e correlacionou o conjunto de dados informativos obtidos, formulando conteúdo de

relevo para a tomada decisão, transitando de dados informacionais inconsistentes para conhecimento mais consolidado.

Enquanto conceito, a inteligência deverá ser analisada em três prismas. Enquanto *processo*, enquanto *produto* e enquanto *organização*. Enquanto *processo*, que irá ser aprofundado seguidamente, a inteligência é a informação (tendencialmente o conjunto destas) que é requerida, pesquisada, analisada e disseminada, coadjuvando o decisor na tomada de decisão. Enquanto *produto*, a inteligência é o resultado do processo anteriormente descrito, das operações desenvolvidas e da análise posterior. É o resultado da correlação entre informações. Enquanto *organização*, a inteligência poderá ser percebida como as unidades/organizações que promovem todo o processo com vista à obtenção do produto inteligência (Lowenthal, 2003, p. 9). Sherman Kent (1967, p. 8) categoriza também a inteligência enquanto *atividade* (a procura de uma determinada espécie de conhecimento) e também enquanto *fenómeno* (o conhecimento resultante dessa mesma atividade).

Quanto ao seu enfoque, a inteligência poderá ter uma natureza *estratégica* ou *tática*⁷. A inteligência *estratégica* tem natureza prospetiva e uma aplicação temporal de médio a longo prazo, onde, perante a intenção de prossecução dos objetivos de dada organização, se identificam as possibilidades e tendências emergentes, podendo assim estimar as alterações no ambiente externo, identificando que consequências poderão ter naquela (Fernandes L. F., 2014, p. 102). É a inteligência requerida para a formulação de políticas e para o planeamento militar, ao nível nacional e internacional (Goldman, 2006, p. 127). Esta não lida com alvos individuais, mas sim com tendências ou fenómenos, que podem ser interpretados através da observação de um espectro alargado de atividades associadas (McDowell, 2009, p. 17).⁸

7 Também poderá ser designada de inteligência *operacional*, apesar de alguns autores considerarem que são duas tipologias díspares.

8 Segundo Romana (2005, p. 5), esta pode ainda assumir distintas vertentes: a *política*, a *de defesa* ou a *de segurança*. A inteligência estratégica *política* pode ter um carácter *ofensivo* ou *defensivo*. É *defensiva* quando a componente trabalhada é a identificação de vulnerabilidades, a prevenção e a neutralização de ameaças conduzidas por agentes e entidades contra os interesses externos (permanentes ou conjunturais) de um determinado Estado. É *ofensiva* quando a produção de inteligência assenta essencialmente na contribuição para a execução de estratégias visando projetar interesses (permanentes ou conjunturais), influenciar, determinar e condicionar o quadro geopolítico, geoeconómico e geocultural de espaços tidos como vitais. A inteligência estratégica *de defesa* que, por sua vez, é um subsistema da inteligência estratégica *política*, sendo as primeiras definidas pela necessidade de os Estados possuírem uma avaliação do potencial estratégico de defesa de determinados países, alianças e organizações, considerados como focos de hostilidade. A inteligência estratégica

A inteligência *tática* refere-se aos eventos e condições em teatros de operações específicos, designada pelos comandantes militares como consciência situacional (Johnson L. K., 2007, p. 1). Segundo Jan Goldman (2006, p. 130), é aquela que é necessária para a condução de operações táticas, usada na tomada de decisão específica com vista à resolução de problemas, lidando esta com ocorrências ou crises imediatas. O mesmo autor define ainda (2006, p. 105) a inteligência *tática* como a de curto-prazo, necessária ao planeamento e execução das operações inerentes à segurança nacional. Esta foca-se nas atividades organizacionais imediatas, de rotina e em curso, suprimindo as necessidades dos decisores de “primeira linha e dos supervisores” (McDowell, 2009, p. 13). Em suma, a inteligência *estratégica* e a *tática* diferem somente no alcance, no ponto de vista e no nível de emprego (Goldman, 2006, p. 130).

Quanto à inteligência enquanto produto, esta pode assumir quatro formatos: inteligência *atual*, *prospetiva*, de *alerta* ou de *pesquisa*. A inteligência *atual* aborda os eventos do dia-a-dia, informando os consumidores sobre novos desenvolvimentos (englobando os antecedentes enquadradores), avaliando a sua relevância e alertando sobre as suas implicações a curto prazo. A inteligência *prospetiva* olha para o futuro, procurando aceder a potenciais desenvolvimentos de determinadas matérias, explorando o desconhecido e incognoscível. A inteligência de *alerta* faz “soar alarmes”, avisando os decisores de futuras ocorrências urgentes e que implicarão uma resposta decisória também urgente. A inteligência de *pesquisa* é apresentada em monografias ou em estudos aprofundados, sustentando tanto a inteligência *atual* como a de *prospetiva* (ITTACG, 2009, pp. 12-13).

Em síntese, a inteligência, no plano securitário (a abordada nesta investigação), visa o conhecimento do adversário, não descurando o da conjuntura interna, procurando minimizar o grau de incerteza inerente à tomada de decisão, tornando-a mais eficaz, conduzindo a uma redução de erros cometidos. A sua finalidade não será a obtenção do sucesso pleno, pois este seria utópico, mas sim a limitação máxima dos fenómenos associadas ao insucesso.

de segurança estuda e avalia riscos e previne ameaças, no plano externo ou interno, à segurança dos Estados, enquadrando-se na tipologia de ameaças assimétricas, como é exemplo o terrorismo.

1.3.2. O CICLO DE PRODUÇÃO DE INTELIGÊNCIA

Com vista à obtenção do “conhecimento”, que irá sustentar a tomada de decisão, limitando a incerteza inerente a esta, dever-se-á desenvolver um conjunto de atividades conducentes a esse “conhecimento”. Estamos perante a inteligência enquanto *atividade*. A *atividade* é o processo que se refere aos vários passos e fases da produção de inteligência, desde a percepção da necessidade de conhecimento por parte dos decisores, até à difusão, para aqueles com necessidade de conhecer, dos produtos gerados pela análise. (Lowenthal, 2003, p. 41) “A atividade de informações envolve um processo complexo de pesquisa, avaliação, análise, integração e interpretação de informações” (Cardoso, 2004, p. 150). Esta atividade é também designada por “ciclo de produção de inteligência”.

O ciclo de produção de inteligência assume diferentes fases interligadas e não estanques no seu sentido. Esta afirmação é consensual entre distintos autores. Os modelos apresentados, o número de fases e a sua tipologia é que diferem. Apesar da maioria dos autores defender um ciclo de produção de inteligência de cinco fases, a do *planeamento e direção*, a de *pesquisa*, a de *processamento*, a de *análise* e a de *disseminação* (Phythian, 2013, pp. 1-3), ir-se-á abordar abaixo, pormenorizadamente, o modelo de Lowenthal.⁹

Este afirma que se devem considerar sete fases distintas, a fase dos *requisitos*, a de *pesquisa*, a de *processamento e exploração*, a de *análise e produção*, a de *disseminação*, a de *consumo* e a de *feedback* (Lowenthal, 2003, p. 52). O autor altera ligeiramente algumas das designações das cinco fases convencionais (mas que no fundo as define, quanto ao seu conteúdo, de uma forma semelhante), introduzindo no ciclo as duas últimas fases. Releva o consumo da inteligência e o *feedback* que os consumidores deverão proporcionar aos intervenientes/criadores do ciclo de produção de inteligência.¹⁰

⁹ Existem ainda outras versões do ciclo de produção de inteligência, nomeadamente com quatro fases, onde o procedimento cronológico é o mesmo, diferindo apenas na fragmentação de etapas. É exemplo disso o modelo militar britânico, apresentado pelo *Army Field Manual, Part 3 – Intelligence, Surveillance, Target Acquisition and Reconnaissance* (ISTAR), dividindo o ciclo de produção de inteligência nas fases de *direção*, *pesquisa*, *processamento* e *disseminação* (British Army, 2002, p. 29).

¹⁰ Independentemente do número de fases ou tipologias atribuídas a cada uma delas, os fatores que o tornam o ciclo de produção de inteligência ou mais ou menos eficaz “são a presciência dos decisores, a qualidade dos analistas, a fiabilidade das fontes e a capacidade de os sistemas informáticos registarem, integrarem, cruzarem e disponibilizarem informação de um forma simples e rápida” (Graça, 2010, p. 218).

1.3.2.1. Requisitos

A fase dos *requisitos*, conceptualmente abordada por Lowenthal, é também usualmente designada de “planeamento e direção”. Aqui, o ciclo de produção de inteligência surge em função das necessidades da organização/pessoa, sendo que deverá ser essa mesma organização (encabeçada pelo decisor) a definir hipóteses em função de um determinado problema. Ou seja, transmitir aos intervenientes no ciclo qual a inteligência que necessita. Aqui são identificados os problemas ou assuntos que os consumidores (decisores) consideram que devem ser objeto das suas atividades de inteligência, devendo ser identificadas as suas necessidades, seja ao nível estratégico ou operacional, conduzindo assim aos objetivos almejados (Fernandes L. F., 2014, pp. 106-107).

Nesta primeira fase, num plano governamental, os gestores do ciclo (oficiais de inteligência) e decisores políticos deverão decidir quais as informações que deverão ser recolhidas, fornecendo assim ao principal decisor executivo, e outros com influência no processo de tomada de decisão, conhecimento, idealmente prospetivo (Jonhson, 2009, p. 35). “Os decisores devem pois estar posicionados no centro da dinamização do *intelligence cycle*” (Graça, 2010, p. 218), sob pena de existirem distorções resultantes de falhas de comunicação com os profissionais de inteligência, sendo o processo de pesquisa e produção mal direcionada. (Jonhson, 2009, p. 35).¹¹

Quanto aos tipos de requisitos (de pesquisa e de produção de inteligência), estes dividem-se em três distintos: os *orientados pelos analistas*, os *orientados pelos eventos* e os *agendados*. Os primeiros são baseados no conhecimento dos consumidores e do problema, os segundos surgem em resposta a eventos relevantes temporalmente próximos e os terceiros relacionam-se com atividades periódicas com necessidade de documentação e atualização de estado. No que diz ainda respeito ao consumidor de inteligência, os requisitos poderão ter uma natureza

¹¹ De modo a resolver o problema apresentado, os decisores e os produtores de inteligência, que deverão encontrar-se em plena articulação (o aspeto de maior relevância para Krizan), colocarão seis perguntas chave, que representam o problema de inteligência: “quem”, “o quê”, “quando”, “onde”, “porquê” e “como”. Essas responderão às necessidades de inteligência. Permitirão que os decisores e analistas conheçam as suas carências e as suas capacidades em relação a um cenário de inteligência específico, estabelecendo aspetos orientadores que permitirão delinear uma estratégia de pesquisa, sendo consequentemente crucial na condução de um eficiente esforço de produção (Krizan, 1999, pp. 13-16).

de curto prazo (*ad hoc*) ou de longo prazo (permanente), quanto à oportunidade, e uma natureza ampla (estratégica) ou limitada (tática), quanto ao alcance (Krizan, 1999, p. 18).

1.3.2.2. Pesquisa

A *pesquisa* é a atividade que pode ser caracterizada como “um processo dinâmico e contínuo de exploração sistemática das origens de dados e informações” (Fernandes L. F., 2014, p. 110) pelos órgãos de pesquisa, com o objetivo de dar resposta ao problema e consequente hipótese/s levantadas na fase anterior. A função da *pesquisa* baseia-se na procura, correspondendo aos objetivos de inteligência validados e às fontes de informação disponíveis, com o resultado dessa conexão ser a transformação de dados informativos em informações utilizáveis (Krizan, 1999, p. 21).

Os dados informacionais são obtidos através de múltiplas formas de recolha, sendo estas movidas por dois fatores, a natureza das informações procuradas e a capacidade de adquiri-las de várias formas. Essas várias formas são designadas de “INTs” (Lowenthal, 2003, p. 54). As “INTs”, também reconhecidas como “fontes”, poderão ser classificadas, de grosso modo, como *abertas* ou *classificadas*. Segundo Fernandes (2014, p. 110), as *abertas*, como o próprio nome indica, são exploradas pela via regular, sem constrangimentos, no que ao acesso diz respeito (do ponto de vista do comum cidadão), como serão exemplos os meios de comunicação social ou a própria *internet*. As *classificadas* poderão ser fragmentadas em *oficiais* (relatórios de entidades públicas com determinado grau de classificação) ou *não oficiais*¹².

Independentemente da segregação entre categorias ou de disciplinas de pesquisa de informações, como irão ser abordadas seguidamente em pormenor, o objetivo da comunidade de inteligência será produzir *all sources intelligence*, em regime de fusão. A inteligência deverá surgir do maior número possível de fontes de pesquisa, compensando assim as deficiências de cada uma, lucrando o ciclo de produção de inteligência com sua força combinada (Lowenthal, 2003, p. 55).

¹² Que poderão ser *voluntárias*, como será exemplo um arrendido ou uma testemunha, ou *pagas*, como serão os informadores (Fernandes L. F., 2014, p. 110)

Estruturalmente, as disciplinas de pesquisa de informações, dividem-se essencialmente em dois grandes blocos: a pesquisa humana e a pesquisa técnica, usualmente designadas por *Human Intelligence* (HUMINT) e *Technical Intelligence* (TECHINT)¹³. A primeira é aquela que surge a partir da atividade de onde é utilizada como principal forma de pesquisa os sentidos dos seres humanos e a segunda é da pesquisa de dados com recursos a máquinas (Fernandes L. F., 2014, p. 111)¹⁴. Apesar de, separadamente, estas duas formas de explorar as fontes facultarem distintos tipos de informação, elas deverão ter um papel complementar, servindo assim o ciclo de produção de inteligência de um modo mais eficaz (Shulsky & Schmitt, 2002, p. 37).

A TECHINT divide-se em três sub-blocos disciplinares. A *Signals Intelligence* (SIGINT), a *Imagery Intelligence* (IMINT) e a *Measurement and Signature Intelligence* (MASINT). A SIGINT é o termo genérico dado ao processo de extrair informações de ondas eletromagnéticas interceptadas, geralmente denominadas de sinais. A extração pode ocorrer pela via da intercepção e desvio de comunicações externas, através das referidas ondas eletromagnéticas ou outro meio de transmissão (subdisciplina da *Communications Intelligence*, ou COMINT). Pode ocorrer através da intercepção, processamento e análise de telemetria externa, nomeadamente no âmbito da transmissão de sinais de rádio associados a sensores de bordo de veículos aeroespaciais, reveladores das suas características de voo e de desempenho (subdisciplina da *Telemetry Intelligence*, ou TELINT, também conhecida por *Foreign Instrumentation Signals Intelligence*, ou FISINT). Também poderá ocorrer pela via da intercepção, processamento e análise de radiações eletromagnéticas, não relacionadas com comunicações, provenientes de equipamentos militares, como será exemplo disso os radares (subdisciplina da *Electronic Intelligence*, ou ELINT) (Shulsky & Schmitt, 2002, p. 27).

A IMINT, também referida como *Photo Intelligence* (PHOTINT), é a forma de recolha de informações pela via da imagem fotográfica, através de sistemas óticos ou eletro-óticos, extraída pela utilização de satélites ou veículos aéreos, tripulados ou não tripulados

¹³ Consultar Anexo II, onde se poderá compreender, organicamente, as disciplinas de pesquisa de informações.

¹⁴ Segundo Krizan (1999, p. 23), as fontes ainda podem ser estruturalmente divididas em quatro distintas categorias que, por sua vez, poderão abarcar diversas disciplinas de pesquisa de informações (anteriormente introduzidas como “INTs”). As categorias de fontes são: pessoas, objetos, emanações e registos. A primeira visa extrair informações de seres humanos com conhecimento direto ou indireto dos factos, a segunda de características físicas de equipamentos, materiais ou produtos, a terceira detetar fenómenos causados pela natureza ou pelo homem e a quarta obter informações de relatórios simbólicos, não simbólicos ou numéricos.

(Lowenthal, 2003, p. 65)¹⁵. Derivada da IMINT, a *Geospatial Intelligence* (GEOINT) é a inteligência resultante da exploração de imagens e informações geoespaciais que permitem descrever, avaliar e representar visualmente recursos físicos e atividade geograficamente referenciadas na Terra (ITTACG, 2009, p. 7).

A MASINT é a recolha científica e técnica de informações obtidas pela análise quantitativa e qualitativa de dados (métricos, angulares, espaciais, de comprimento de onda, entre outros) provenientes de sensores técnicos, com o objetivo de identificar quaisquer características distintivas associadas à fonte, emissor ou remetente, facilitando a identificação desta. (ITTACG, 2009, p. 7) Essencialmente, a MASINT deve ser entendida como toda a restante TECHINT, que não seja SIGINT ou IMINT, nomeadamente incluindo as categorias de radar, geofísica, infravermelhos, radiação nuclear, entre outras (Richelson, 2007, p. 112).¹⁶

Como disciplina díspar das anteriores, não diretamente encaixada na HUMINT, ou na TECHINT, mas sendo complementar e por diversas vezes ignorada da utilização dessas duas, a *Open-Source Intelligence* (OSINT) é a informação não classificada com potencial valor de inteligência e que está disponível para o público em geral. (ITTACG, 2009, p. 7). Williams & Blum (2018, p. 7) afirmam, no entanto, que OSINT é diferente de *Open-Source Information* (OSIF), pois a segunda é meramente informação desclassificada e disponível ao público, enquanto a primeira já são os resultados da aplicação de um processo de exploração da OSIF, validando-a como relevante, precisa e utilizável pelos consumidores¹⁷.

1.3.2.3. Processamento e Exploração

As informações recolhidas pelos meios técnicos não transitam da fase de *pesquisa* em formatos passíveis de serem automaticamente analisados. Estes deverão ser processados e explorados de modo a poderem migrar para a fase seguinte (Lowenthal, 2003, pp. 45-46). É uma fase pré-analítica onde a informação crua é filtrada e tornada inteligível para a análise,

¹⁵ Este método usa a recolha de fotografia a longa distância, obtendo assim imagens de sítios ou coisas não visualizáveis por outra via (Shulsky & Schmitt, 2002, p. 22).

¹⁶ Alguns autores inserem a MASINT na disciplina SIGINT, considerando a primeira uma subdisciplina, um produto, ou mesmo um subproduto da segunda (Lowenthal, 2003, p. 73).

¹⁷ É hoje consensual que a OSINT assume uma posição preponderante no ciclo de produção de inteligência, sendo a *internet* um elemento essencial neste contexto, associado aos motores de busca cada vez mais especializados e eficazes, permitindo ultrapassar barreiras geográficas e horárias (Graça, 2010, p. 222).

sendo esta, essencialmente, uma fase técnica (Phythian, 2013, p. 3). Independentemente do tipo de pesquisa desenvolvida anteriormente, as informações recolhidas deverão ser catalogadas de modo coerente, antes do processo de produção de inteligência, dando-lhes um formato utilizável e munido de significado, quando este não era evidente nas informações originalmente pesquisadas (Krizan, 1999, p. 25).

Ações como as de interpretar o conteúdo de imagens provenientes da IMINT, descortinando o que elas possam representar, ou traduzir conteúdos provenientes da COMINT ou da OSINT, que se encontra em língua díspar da dominada pelo analista¹⁸, representam a função da fase de *processamento* (Johnson L. K., 2007, p. 41). Seguidamente, e ainda nesta fase, as matérias pesquisadas são agrupadas por categorias, empregando, eventualmente, bases de dados eletrónicas, existindo compilações por padrões (ainda embrionários). No entanto, o agrupamento eficaz deverá ser impessoal, imparcial, pragmático e objetivo, estando livre de preconceitos na integração das informações (Krizan, 1999, p. 26).

Na fase do *processamento* também a relevância e o valor das informações recolhidas são avaliados. A informação da fonte deverá ser examinada assim como a sua aplicabilidade no processo de produção de inteligência. Deverão ser tidos em consideração três aspetos neste âmbito: a *confiabilidade*, a *proximidade* e a *adequação*. A *confiabilidade* da fonte, no que diz respeito à precisão das informações extraídas no passado, influencia essa precisão e também a sua credibilidade. A *proximidade* diz respeito ao contacto que a fonte tem com a informação, sendo, naturalmente, uma fonte primária mais credível do que outra, ou seja, quantos mais passos existirem entre a informação e a fonte, maior será a probabilidade de distorção dessa informação. A *adequação* está relacionada com o grau de conhecimento que a fonte tem sobre a matéria que está a informar, tornando-a mais credível se dominar a temática específica relatada (Krizan, 1999, pp. 26-27)¹⁹.

¹⁸ Serão exemplos desta fase a transcrição de escutas telefónicas e a tradução de notícias provenientes do estrangeiro.

¹⁹ Fernandes (2014, p. 116) indica que é nesta fase que se avaliam a confiança das fontes e a verosimilhança das informações, propondo uma matriz de avaliação de duas colunas, onde na primeira consta o grau de confiança das fontes, que varia entre seis graus (“A – Absolutamente segura”; “B - Normalmente segura”; “C – Razoavelmente segura”; “D - Normalmente não segura”; “E - Não segura”; e “F – Não pode ser apreciada”). Na segunda coluna consta o grau de verosimilhança da informação, que similarmente varia entre o mesmo número de graus (“1 – Informação confirmada por outras fontes”; “2 – Informação provavelmente verdadeira”; “3 –

1.3.2.4. Análise e Produção

“*The ultimate goal of intelligence is accurate analysis. Analysis is not, however, an exact science and there have been, and undoubtedly will continue to be, failures by analysts to prepare accurate and timely assessments and estimates.*” (Best Jr., 2010, p. 40)

A análise de informações consiste no processo de avaliar e transformar dados informacionais simples em descrições, explicações e conclusões para os consumidores de inteligência (Berkowitz & Goodman, 1989, p. 85). Refere-se ao processo de transformar fragmentos de informações que foram recolhidos (independentemente do método) em algo que será utilizado pelos decisores políticos e comandantes operacionais. A fase da *análise* é, na realidade, uma dupla fase, onde as informações pesquisadas e processadas anteriormente, serão primeiramente analisadas e posteriormente utilizadas na produção de inteligência. Nesta fase (na realidade duas fases) ocorrerá a integração, a avaliação de confiabilidade²⁰, a validação e a atribuição de relevância dos dados (análise, propriamente dita). Posteriormente ocorrerá a produção, a (eventual) revisão pelos pares e a revisão de supervisão (Johnston & Johnston, 2005, p. 48).

Aqui o objetivo será revelar a um decisor específico o significado subjacente às informações sobre um alvo selecionado, não sendo meramente a reorganização de dados e informações num novo formato, devendo ser descrito o fenómeno e o maior número possível de variáveis relevantes, interpretando significados e efeitos do fenómeno (Krizan, 1999, p. 29). “É um processo de índole científica, sujeito a um conjunto de parâmetros metodológicos, que visa prioritariamente o *conhecimento do que está a acontecer* e idealmente a excelência da *capacidade prospetiva*” (Graça, 2004, p. 430).

No processo de análise de informações a objetividade deverá ser fator primordial a ter em consideração, sendo que o raciocínio inerente a esta fase deverá ser cumulativamente indutivo, dedutivo, abduutivo e científico (Krizan, 1999, p. 30). Deverá focar-se na evidência,

Informação possivelmente verdadeira”; “4 – Informação duvidosa”; “5 - Informação de verosimilhança improvável”; “6 – Informação cuja verosimilhança não pode ser apreciada”).

²⁰ Alguns autores consideram que esta avaliação ocorre previamente, na fase do *processamento*.

sustentadora das hipóteses específicas trabalhadas, sendo esta a força probatória, traduzindo pragmatismo e sensibilidade observativa (Moore, 2007, p. 55).²¹

1.3.2.5. Disseminação e Consumo

Na fase da *disseminação* ocorre a distribuição do produto inteligência aos consumidores, garantindo o respeito pelos princípios do direito de conhecer e da necessidade de conhecer (Fernandes L. F., 2014, p. 123). A difusão do conhecimento produzido no curso do ciclo de produção de inteligência deverá chegar àqueles que efetivamente deverão conhecer, a fim de decidir, num plano estratégico ou tático, e não àqueles que, apesar de poderem estar munidos de um significativo grau de credenciação²², não serão os consumidores que o gestor do ciclo deseja que sejam.

Nesta fase, segundo Lowenthal (2003, p. 49), existem alguns aspetos que deverão ser tidos em consideração aquando da difusão do produto inteligência. Considerando a vasta quantidade de informações coletadas e produtos de inteligência gerados, dever-se-á apurar o que é realmente relevante a ser reportado. Dever-se-á ter certezas quanto à amplitude da ação de difusão, nomeadamente no que diz respeito aos patamares decisórios, garantindo quem deverá conhecer em concreto. O princípio da oportunidade também é um fator de relevo na tarefa de difundir, procurando que o consumidor receba a inteligência no momento certo (nem com muita antecipação, nem de forma extemporânea).

Existirá importância na definição do detalhe da inteligência difundida, procurando ser sucinto sem excluir aspetos de relevo, ponderando, em função da tipologia de consumidor, a extensão do produto. Por fim, deverá ser avaliada a melhor forma de difusão, no que diz respeito ao

²¹ No que diz respeito às ações a desenvolver, no curso da fase da análise, e no contexto específico das ameaças irregulares, como é o caso do contraterrorismo abordado nesta investigação, Larson, Eaton, Nichiporuk & Szayna (2008, p. xii) sugerem um *framework* de oito fases: 1ª - Avaliação preliminar da situação; 2ª - Identificação da questão central; 3ª - Identificação do *stakeholder*; 4ª - Recolha básica de dados; 5ª - Análise do *stakeholder*; 6ª - Avaliação das ligações/relacionamentos no âmbito da rede do *stakeholder*; 7ª - Avaliação da liderança associada ao *stakeholder*; 8ª - Integração da inteligência, compreendendo o curso provável da ação da ameaça ou o desenvolvimento geral da mesma. Entre a primeira e a quarta fase os autores abordam as fases dos *requisitos* e da *pesquisa*, que irão sustentar a fase de análise, constante entre a quinta e sétima fase, culminando na subfase da análise, a produção, no oitavo passo.

²² Em Portugal os graus de credenciação (Muito Secreto, Secreto e Confidencial) são previstos pelo SEGNA 1, sendo que o diploma afirma no seu ponto 1.2.2.4. que, independentemente do grau atribuído, “O acesso às matérias classificadas deve restringir-se, exclusivamente às pessoas que tenham necessidade de conhecer para cumprimento das suas funções ou tarefas” (Presidência do Conselho de Ministros, 1988).

formato de relato, adaptando o modelo utilizado às circunstâncias e, uma vez mais, ao consumidor. A difusão poderá assumir a forma de pequenos memorandos, relatórios formais, *briefings* ou outras formas de difusão de inteligência (Shulsky & Schmitt, 2002, p. 41).

O conjunto de preocupações anteriormente elencadas representarão uma maior aplicabilidade, maior credibilidade e maior aproveitamento da inteligência produzida. O valor do produto da análise de inteligência não deverá ser somente medido pela sua qualidade e precisão, mas sim pelo valor que é atribuído pelo decisor (Marrin, 2007, p. 199). Daí a importância da disseminação eficaz.

1.3.2.6. *Feedback*

Lowenthal (2003, p. 50) considera que a fase de *feedback* deve ser olhada de forma autônoma, não sendo esquecido o papel que os consumidores deverão ter no curso do ciclo de produção de inteligência. Idealmente, os decisores dariam continuamente *feedback* aos envolvidos no ciclo, transmitindo os aspectos que estavam a ser úteis, ou não, que áreas necessitariam de incremento, redução ou continuidade no empenhamento, entre outras observações. O *feedback* deverá ser capaz de fazer regredir o ciclo, se necessário, para qualquer fase, inclusivamente para a dos requisitos. A intervenção do decisor/consumidor poderá promover uma redefinição de planeamento e de pesquisa, um aprimoramento do processamento e exploração das informações recolhidas, a reanálise daquilo que anteriormente foi selecionado e consequente produção, díspar da anterior.

No entanto, na realidade, segundo o autor, os produtores recebem menos *feedback* do que o desejável, não sendo sistemática essa interação. “*The failure to provide feedback is analogous to the policymakers’ inability or refusal to help define requirements*” (Lowenthal, 2003, p. 52). O alheamento do consumidor será uma das causas de eventuais fracassos do ciclo de produção de inteligência. O *feedback* não deverá ser um componente do processo de produção de inteligência, reservado exclusivamente para a revisão dos resultados estratégicos das posteriores medidas do decisor (Ross & Duchesne, 2007, p. 33), devendo ter uma aplicação intra-processual e interventiva.

2. O FENÓMENO DO TERRORISMO

2.1. O CONCEITO DE TERRORISMO

O terrorismo é um ato subversivo que visa anular ou fragilizar o poder instituído numa determinada sociedade. Assim sendo, não se poderá analisar o conceito de terrorismo sem antes compreender os de sociedade, poder e subversão.

A sociedade é um agrupamento de seres humanos, com caráter durável, tendo um espaço territorial, onde permanece. Para a sua existência, deverá verificar-se a continuidade, a complexidade de relações (que individualiza, a cada momento, a fase histórica da mesma sociedade), a unidade operatória (os indivíduos integrados deverão submeter-se às leis do seu funcionamento) e a diferenciação das participações individuais (resultante das diversidades fisionómicas, psíquicas, técnicas, culturais, entre outras) (Soares, 1975, p. 50). Este agrupamento de seres humanos também poderá ser designado de povo, pois é um todo, “dotado de unidade na sua diversidade”, unido “pela utilidade comum e pelo consenso do direito, aquilo a que chama de república, ou grei” (Maltez, 2018, p. 359).

A gestão da sociedade implica a aplicação de regras de conduta, escudadas no direito (que a própria sociedade de modo consensual, ou não, criou), sendo essa aplicação designada de exercício de poder. O poder, independentemente da sua *forma*, *sede* ou *ideologia* (perspetiva tridimensional apresentada por Moreira (2014, p. 127)) é um poder coletivo através do qual se expressa a *polis*. “É um todo que pode ser mais do que a soma das respetivas parcelas, sendo também o “elástico” que integra e coordena os mais variados poderes” (Maltez, 1996, p. 122). O poder, “enquanto *capacidade criada por um acordo social*, não se confunde com a simples *coerção*” (Maltez, 1996, p. 119). Noutra perspetiva mais funcional, podemos afirmar que o poder pode ser definido como o “conjunto de meios capazes de coagir os outros a um determinado comportamento” (Lara, 2015, p. 259).

Associado ao exercício do poder, existe o conceito de legitimidade, sendo esta a “relação da conformidade entre a origem e a conduta do poder disposto em regras morais ou religiosas cruciais para grupos sociais estabelecidos” (Lara, 2015, p. 260). Associado ainda ao poder e à legitimidade do exercício deste, surge a obediência. A obediência ao poder legítimo. A força e

o poder são, acima de tudo, “mais uma *relação* do que apenas uma *estrutura*, e depende da extensão da obediência consentida” (Moreira A. , 2014, p. 148). “O poder é, assim, considerado essencialmente como um atributo exclusivo do ser humano, como um domínio caracterizado pela posse e como uma capacidade que, entre outras, se desenvolve no sentido da realização de um objetivo, da concretização de uma finalidade” (Santos, 2007, p. 241).

Por sua vez, de modo a destronar o poder instituído, a subversão é “toda a ação de alcance político-social desencadeadora de um processo de mudança rápida, de afetação social ampla e profunda, geralmente desencadeadora de reações em cadeia, com a finalidade de atingir o ponto de rutura de um determinado sistema social e conseqüente situação de desorganização social” (Lara, 2015, p. 306). Usualmente não tem “periodicidade certa e determinável, e utilizando modelos afins, todos eles caracterizados pela forma ilegal de intervenção, com intenção premeditada a uma alteração profunda de uma determinada conjuntura” (Lara, 2015, p. 306). “É sempre considerada transitória, passageira, sendo um instrumento fundamental da ação, fatalidade insuperável, ou de outro qualquer sentido, mas sempre numa linha de instrumentalidade e de precaridade” (Lara, 2015, p. 306). Os métodos/táticas de subversão poderão ser o golpe de Estado, a guerra civil, a revolução, a guerrilha ou o terrorismo (Lara, 2011, p. 53).

O terrorismo, enquanto conceito, apesar de ser provavelmente dos mais politizados atualmente no panorama da política internacional, continua a ser um conceito contestado, dada a inexistência de concordância entre as pessoas, no que diz respeito ao seu significado ou com o escopo desse significado. O medo e a violência utilizados no âmbito deste método subversivo, considerado ilegítimo por uns (defensores da ordem instituída), e por outros, legítimo, sendo os atores destes atos vistos como revolucionários, lutadores da liberdade, mártires, resistentes ou mesmo soldados (Schmid, 2011, p. 40). “One man’s terrorist is another man’s freedom fighter” (Laqueur, 1987, p. 7).

O terrorismo é “instrumento de grupos minoritários e ativistas, que procuram a destruição da capacidade do aparelho do poder de governar a sociedade civil pelo facto de o impedirem de oferecer a esta segurança da vida quotidiana. Acreditam que o descrédito do aparelho do poder terá como contrapartida o desencadear do processo de transferência da obediência para o aparelho revolucionário que pretendem instalar” (Moreira A. , 2014, p. 183). É um ato

político subversivo, instrumental (é um meio e não um objetivo final) e com propósitos mediatos ou imediatos (Lara, 2015, p. 348). “É sempre uma arma de quem não tem outros meios, legítimos, desde logo, mas também subversivos, para impor rapidamente a sua vontade” (Lara, 2002, p. 49). Inevitavelmente, o terrorismo foca-se no poder: perseguição do poder, aquisição do poder e o uso do poder para alcançar a mudança política. Não exclui, no entanto, a utilização da violência ou ameaça da sua utilização, usada e direcionada na busca, ou a serviço de um dado objetivo político (Hoffman, 2006, p. 3).

Relativamente à sua classificação, o terrorismo poderá ser *indiscriminado* ou *seletivo* (Lara, 2015, p. 440). Os atentados que visem lesar destinatários indefinidos, aleatórios, onde são irrelevantes os danos colaterais e onde as vítimas podem ser alheias às causas defendidas pelo agente subversivo ou pelo conservador da ordem instituída, são tipificados como *indiscriminados*. São enquadrados no terrorismo *seletivo* as ações direcionadas a uma determinada individualidade, individualidades ou a uma determinada organização. A classificação de *indiscriminado* pode ainda ser dividido em três subtipos, o *indiscriminado convencional*, o *super-terrorismo* e as *ações de apoio e financiamento do terrorismo*.²³

Quanto à evolução e funcionamento do terrorismo, este surge pelo descrédito da ordem instituída, do poder político. Desenvolve-se, então, uma intenção e consumação da desobediência ao poder político, que resulta numa transferência progressiva da obediência para o poder errático. No apoio a este poder, subversivo, existe o reconhecimento do mesmo como parceiro, legitimando-o, seguidamente. Após todo este processo, é intenção das forças subversivas, utilizadoras do terrorismo, que exista uma destituição do poder instituído e substituição. A alternativa aceite será a negociação e a cedência, impondo assim os ideais defendidos (Lara, 2011, p. 57). O terrorista usa a violência contra poderes ideológicos, de

²³ O primeiro corresponde ao descrito anteriormente (terrorismo que utiliza meios usuais, de regular significância, em matéria de lesões à vida, integridade física ou património) enquanto, o *super-terrorismo* surge quando a indiscriminação do atentado se perpetua mediante a utilização de meios anormalmente letais e danosos, assumindo proporções alarmantes, afetando psicologicamente as vítimas e os expetadores (Lara, 2007, p. 46). Este *super-terrorismo* pode assumir a forma de ataques nucleares, químicos, biológicos, ações suicidas de larga escala e até o ciberterrorismo. O último instrumento terrorista, afeto ao *super-terrorismo*, poderá ser perpetuado de forma direta ou indireta. Diretamente pela ação de *hackers* na intrusão ou destruição de redes estratégicas ou indiretamente, mediante a propaganda de ideologias e intenções, formação técnica e tática (fabrico de explosivos, por exemplo) e divulgação de sites de venda de "utensílios" necessário à consumação de atentados. As ações de apoio e financiamento do terrorismo poderão surgir perante o apoio de determinados Estados ou da criminalidade organizada (Lara, 2011, p. 55).

forma calculada, e no intuito de produzir choque e medo mediante o seu caracter aparentemente bizarro, casuístico e absurdo. Visa provocar o medo e assim criar uma atmosfera de trauma e caos, produzindo nas pessoas o sentimento de vulnerabilidade, minando a confiança na capacidade protetora dos governos (Dougherty & Pflatzgraff, Jr., 2003, p. 435).

Eu suma, “terrorista” é uma descrição que quase nunca foi voluntariamente adotada por nenhum indivíduo ou grupo. É aplicada por estas a outros, antes de mais pelos governos dos estados que atacam. “Os estados não se têm coibido de rotular os seus oponentes violentos com esse título, com as implicações evidentes de barbaridade, criminalidade e, talvez mais perentoriamente, falta de apoio político real” (Townshend, 2006, p. 9). No entanto, não se poderá alhear a atividade “terrorista” de alguns Estados, nomeadamente aquando da aplicação da violência, e da promessa desta, na execução das suas políticas, contrariamente à vontade do seu povo. Alguns fazem-no pela via do apoio ao terrorismo (ao nível do financiamento, ideológico, militar e logístico), outros dirigem o próprio terrorismo (planeiam e chefiam as ações em si) e os últimos empreendem o terrorismo (envolvendo as suas estruturas oficiais, diplomáticas, de segurança ou de inteligência, em ações terroristas (Ganor, 2002, p. 300).

2.2. O PANORAMA ATUAL DO TERRORISMO

O terrorismo, nos dias de hoje, continua a ser não só uma das maiores preocupações dos Estados, mas também das organizações supranacionais, considerando o carater global, alheio a fronteiras, nacionalidades ou religiões, sendo um desafio que a comunidade internacional deverá combater de modo articulado (NATO, 2019). “O terrorismo tornou-se numa das ameaças centrais debatidas em encontros internacionais de alto nível, em documentos estratégicos nacionais e internacionais, assim como no mundo académico” (Duque, 2016, p. 133).

Tendo por base estatísticas consolidadas, constantes na base de dados *Global Terrorism Database* (GTD)²⁴, que relatam a atividade terrorista mundial, entre os anos de 2001 e de

²⁴ O GTD é um banco de dados de código aberto que inclui informações sobre ataques terroristas nacionais e internacionais em todo o mundo, de 1970 a 2018, incluindo mais de 190000 registos associados ao fenómeno. Para cada evento, são disponibilizadas informações sobre a data e o local do incidente, as armas usadas e a

2018, tem-se verificado um acréscimo significativo do número de atentados terroristas e de mortes e feridos causados por esses atentados, sendo o seu pico de incidência entre os anos de 2014 e 2015. Como se poderá observar no gráfico nº 1²⁵, no ano de 2014 existiram 16.908 atentados, resultando em 44.492 mortes e 41.130 feridos. No ano de 2015, apesar de o número de atentados reduzir em 12% e o número de mortes associadas reduzir também em 13%, o

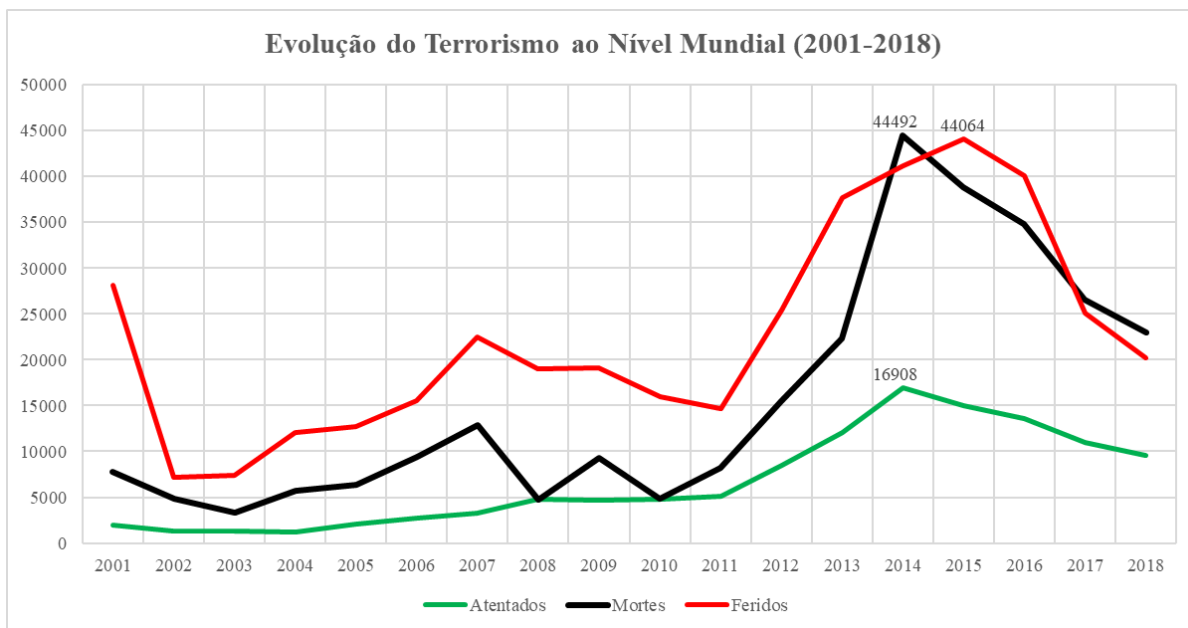


Gráfico 1: Evolução do Terrorismo ao Nível Mundial (2011-2018)

número de feridos aumentou, atingindo o número recorde de 44.064.

De salientar que a última década (2010-2018 – 9 anos contabilizados) teve quatro vezes mais atentados que a penúltima (2001-2009 – 9 anos contabilizados), variando entre os valores de 96.571 para 218.600, e 3,5 vezes mais mortes subjacentes, escalando de 64.153 para 218.600 mortes. Independentemente da significância da década de 2010, os atentados, mortes e feridos correlacionados encontram-se em decréscimo desde o biénio de 2014-2015, sendo que, de momento, e tendo por base valores de 2018 (que na realidade já poderão estar desatualizados) o número de atentados fixou-se nos 9.607, as mortes no valor de 22.987 e os feridos em 20.259.

natureza do alvo, o número de vítimas e, quando identificável, o grupo ou indivíduo responsável. É uma base de dados gerida pela *National Consortium for the Study of Terrorism and Responses to Terrorism* (START) (START, 2019).

²⁵ Poderá ser observado com maior pormenor em Anexo I.

De *grosso modo*, poder-se-á afirmar que atualmente o fenómeno terrorista mundial encontra-se com metade de preponderância que já teve em 2014-2015. No entanto, ressalva-se que continuam a verificar-se valores acima da média do novo milénio e extremamente acima da média geral, no que diz respeito aos registos da GTD desde 1970, consoante se poderá observar no gráfico n.º 2 (START, 2019).

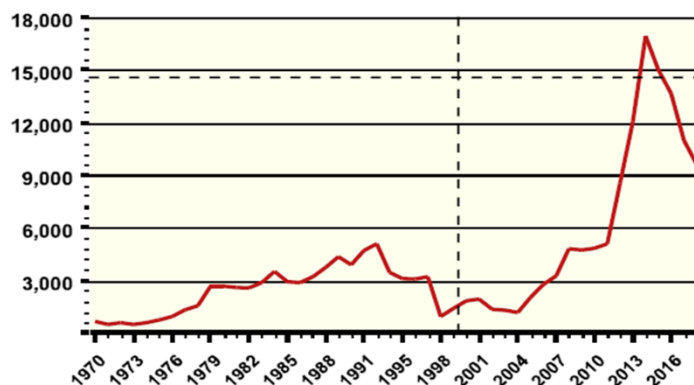


Gráfico 2: Evolução do número de atentados ao nível global.

Considerando o espectro geográfico abordado nesta investigação, onde será abordado o contraterrorismo no eixo anglo-americano, será importante ressaltar que a maioria dos atentados e mortes/feridos subjacentes não ocorreram nesse espaço (entre 2001 e 2018).

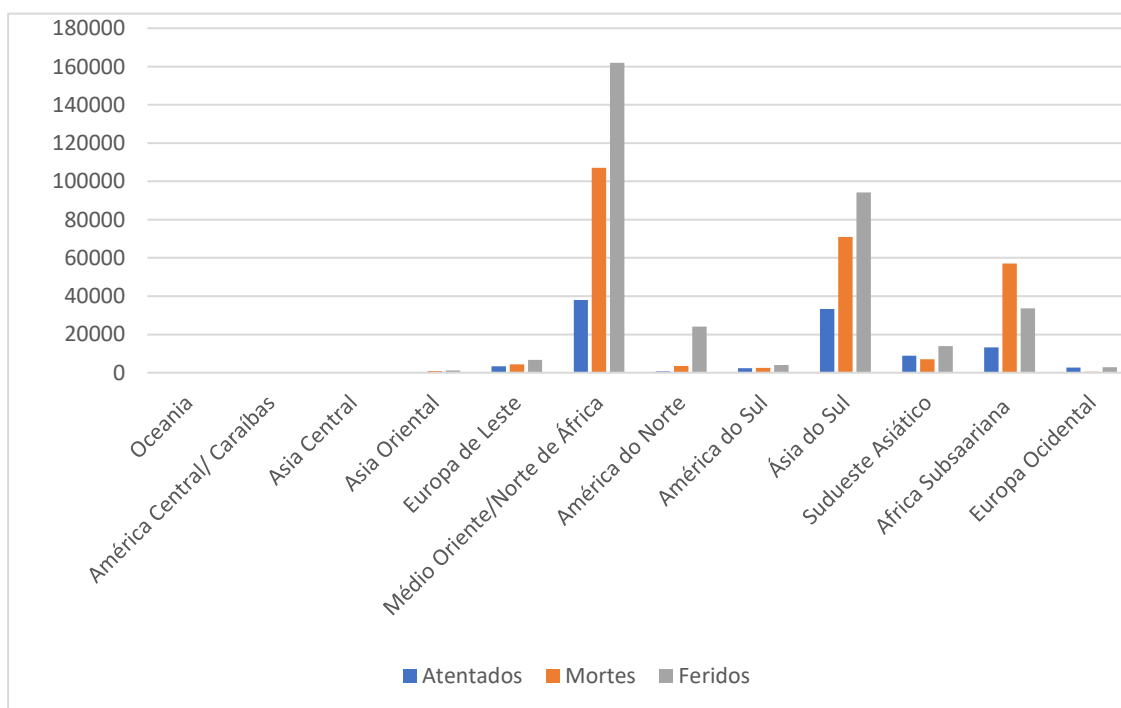


Gráfico 3: Distribuição do número de atentados por região do globo (2001-2018).

Segundo a GTD, e consoante o gráfico nº 3 ²⁶ e constante em Anexo I, as regiões do Norte de África, do Médio Oriente e da Ásia do Sul detêm 73% dos atentados ocorridos em todo o globo, apresentando, cumulativamente, a maioria das mortes e feridos associados (71% e 74%, respetivamente). Países como o Iraque, o Afeganistão e a Nigéria foram os principais promotores da significativa percentagem anteriormente apresentada, ocupando o primeiro, segundo e terceiro lugares, no GTD, num universo de 163 países avaliados (Vision of Humanity, 2019).

Tendo em conta as mencionadas regiões do globo, em geral, e os países relatados, em específico, poder-se-á afirmar que o principal responsável pelo número exacerbado de incidentes e mortes/feridos associados tem sido o terrorismo de matriz islâmica²⁷, nomeadamente correlacionado com os grupos *Islamic State of Iraq and the Levant* (ISIL), *Taliban* e *Boko Haram*, que operaram e continuam a operar com preponderância naqueles espaços geográficos. Com base no GTD, o ISIL perpetuou cerca de 86% dos seus ataques no Iraque, os *Taliban* foram responsáveis por cerca de 60% no Afeganistão e o *Boko Haram* de 50% na Nigéria. Um dos grupos terroristas mais renomados, a *Al Qaida*²⁸, surpreendentemente, no Iraque, Afeganistão e Nigéria (países mais afetados pelo terrorismo) só apresenta cerca de 1,5% dos atentados cometidos, indicando assim que, na realidade, a *Al Qaida* não é dos maiores responsáveis pelo fenómeno terrorista global, no que ao número de incidentes registados diz respeito.

Olhando agora para os países em destaque no âmbito da temática trabalhada, e em contraposição com o relatado nos parágrafos anteriores, o RU e os EUA, desde 2001, representam somente 1,35% do terrorismo mundial (1622 atentados em 119804), no que diz respeito aos incidentes. Relativamente às mortes, estas representam 1,20% (3.504 mortes em 290.176) e aos feridos 6,10% (25.007 feridos em 408.034). De salientar que, no que diz respeito a mortes e ferimentos registados no RU e nos EUA, 86% e 87%, respetivamente,

²⁶ Observável com maior pormenor em Anexo I.

²⁷ Não confundível com o fundamentalismo islâmico. Este trata o regresso às origens do Islão, “apresenta-se como um modelo político e não apenas uma simples visão integrista da religião (...) procuram transformar a lei islâmica num programa sistemático de ideais políticos convertendo-a numa verdadeira Constituição ideológica contemporânea” (Silva T. d., 2016, p. 63).

²⁸ Evitando conflitos de nomenclatura introduzida na base de dados GTD, foram, no Iraque, Afeganistão e Nigéria, assumidos todos o grupo com a designação similar a *Al-Qaeda*, nomeadamente *Al-Qaida* (propriamente dita), *Al-Qaida in Iraq*, *Al-Qaida in the Islamic Magreb* e *Al-Qaida Kurdish Battalions*. Com a designação *Al-Qaeda* não surgiu qualquer resultado.

ocorreram aquando da sequência de atentados a 11 de setembro de 2001, em Nova Iorque, no EUA. Se isolarmos o dia mais singular na história do terrorismo mundial, que é, de sempre, o mais fatídico em termos de mortes e feridos, então poder-se-á observar que os valores causados pela atividade terrorista no RU e nos EUA é perfeitamente residual (0,16% de mortes e 0,76% de feridos).

Abordando agora a evolução do fenómeno terrorista no RU, em específico, poder-se-á observar no gráfico nº4 ²⁹, tendo por base a tabela constante em Anexo I, que o número de incidentes terroristas tem vindo a crescer até 2018, tendo o seu pico de atentados em 2013, com 137 registados, ainda que, no entanto, se têm mantido valores na casa das centenas, contrariamente à tendência mundial, que presencia um decréscimo para metade dos atentados. No que diz respeito às mortes e feridos, o pico mais substancial ocorreu em 2005³⁰(contabilizando 57 mortes e 787 feridos) e o segundo mais significativo em 2017, onde ocorreram 3 principais atentados distintos³¹, (morrendo 42 pessoas e ficando feridas 301, na totalidade dos atentados ocorridos no RU em 2017).

Apesar de os atentados mais mediáticos e com um maior número de mortes no RU estarem associados ao terrorismo de matriz islâmica, não se poderá afirmar que esta tipologia é aquela com maior representatividade, no que ao número de incidentes diz respeito. Entre 2001 e 2018 somente 2% dos atentados terroristas foram associados ao terrorismo de matriz islâmica, sendo que a grande maioria, no RU, estão relacionados com conflitos internos associados à relação entre a Irlanda do Norte e a Grã-Bretanha, nomeadamente no que diz respeito à segregação política, pretendida por alguns cidadãos norte irlandeses, essencialmente dinamizada pelo *Irish Republican Army* (IRA).

²⁹ Pormenorizado na tabela constante em Anexo I.

³⁰ Atentado à bomba ocorrido a 7 de julho de 2005 em Londres, onde 56 pessoas morreram e 784 ficaram feridas, sendo o mesmo reivindicado pela *Al-Qaida*, revelando-se o ataque mais trágico da história do RU (The Guardian, 2019). Salienta-se que a notícia citada do *The Guardian* relata 52 mortes e mais de 900 feridos, enquanto a GTD aborda números díspares.

³¹ Atentados ocorridos em Westminster (Londres), na Manchester Arena (Manchester) e na London Bridge (Londres), totalizando 40 mortes e 217 feridos, sendo um dos ataques reivindicados pelo ISIL, outro cometido por uma só pessoa (que se inspirou no ISIL) e o outro cometido também por uma só pessoa (sem qualquer tipo de afiliações conhecidas (Skynews, 2019)).

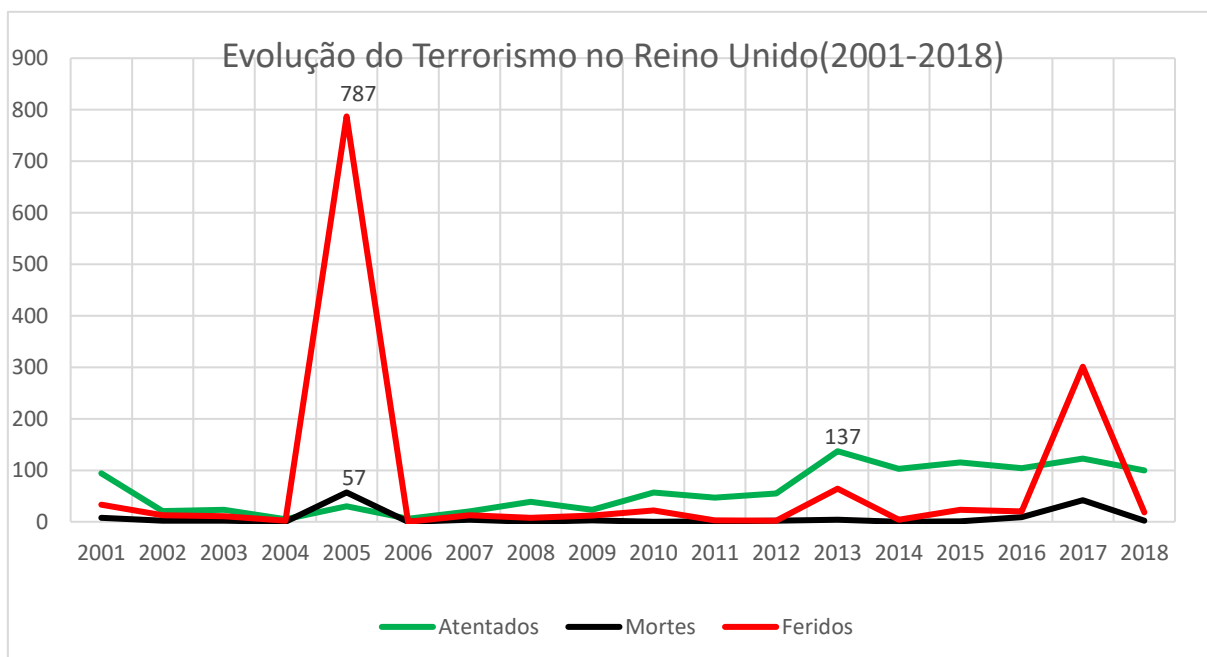


Gráfico 4: Evolução do Terrorismo no Reino Unido (2001-2018)

No espectro norte-americano o cenário é relativamente similar ao do RU, como se poderá observar no gráfico nº5³². O terrorismo nos EUA tem sido oscilante entre os anos de 2001 e 2018, sendo que, nos três últimos anos analisados (2016, 2017 e 2018), tem atingido o maior pico de atentados terroristas, nomeadamente com 67, 66 e 67, respetivamente, representando mais do dobro dos atentados da média do hiato temporal abordado. Apesar de o ano de 2001 ter sido, nos EUA, o mais significativo em termos de fatalidades associadas ao terrorismo, contabilizando 3014 mortes e 21894 feridos (praticamente todos ocorridos no “11 de Setembro³³”), o número de mortes ou feridos correlacionados com o terrorismo, tem-se revelado significativamente baixo, tendo em consideração a população existente nos EUA, cerca de 330 milhões de pessoas (Worldometers, 2019).

³² Pormenorizado em Anexo I.

³³ Conjunto de atentados terroristas em Nova Iorque, Washington D.C. e Pittsburg, ocorridos em 11 de setembro de 2001, causando 3004 mortes e 21871 feridos. Os atentados foram reivindicados pelo grupo terrorista de matriz islâmica *Al-Qaida* (START, 2019).

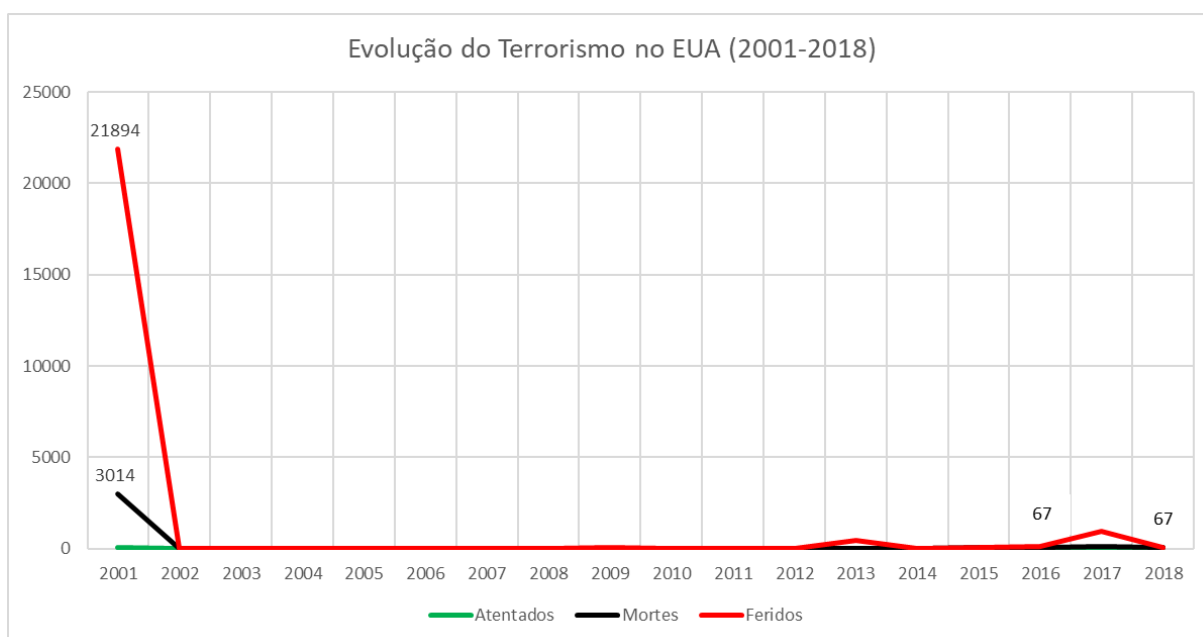


Gráfico 5: Evolução do Terrorismo no EUA (2001-2018)

À semelhança do RU, nos EUA, o atentado terrorista mais significativo, em termos de fatalidades e do conseqüente mediatismo, está associado à matriz islâmica, sendo indubitavelmente o ano de 2001 o mais marcante em todos os aspectos. Outros significantes ocorreram já recentemente, em Orlando (2016)³⁴ e em Las Vegas (2017)³⁵, sendo também estes atentados associados ao terrorismo de matriz islâmica, nomeadamente ao ISIL.³⁶

Em suma, quanto à realidade terrorista no RU e no EUA, é bastante díspar da tendência evolutiva mundial. Globalmente, com forte influência daquilo que vai ocorrendo no Médio Oriente, Norte de África e Sul da Ásia, o fenómeno do terrorismo tem decrescido com alguma preponderância, não deixando, no entanto, de ser preocupante, considerando que os valores mais recentes continuam a ser bastante mais elevados que a média das décadas transatas. O

³⁴ Um atirador ativo de 29 anos de idade disparou contra os frequentadores de uma discoteca gay em Orlando, causando 50 mortes e 53 feridos, em “gesto de lealdade” para com o ISIL. (CNN, 2019)

³⁵ Um atirador ativo de 64 anos de idade matou 59 pessoas e feriu 527 num festival ao ar livre em Las Vegas, não estando associado a qualquer organização terrorista, sendo que, no entanto, o ataque foi reivindicado pelo ISIL (BBC, 2019).

³⁶ No entanto, e tendo por base a GTD, entre 2001 e 2018, somente 9% dos atentados terroristas em território norte americano estão associados ao terrorismo de matriz islâmica. Apesar de a maioria das mortes e feridos serem resultantes de terrorismo de matriz islâmica, o número de atentados não é. Os grupos e as motivações, resultantes em atentados terroristas, nos EUA são altamente diversificados, contrariamente ao RU. Desde grupos associados ao ativismo animal, passando por outros anti-islão, anti-governo ou anti-aborto, a natureza do terrorismo nos EUA não é uniforme, não sendo possível afirmar uma corrente motivacional predominante.

RU e os EUA apresentam-se na fase mais elevada da sua história recente (desde 2001), estando “elevadamente estáveis”, no que diz respeito ao número de incidentes registados.

Quanto ao número de mortes ou de feridos, não é possível afirmar uma tendência crescente ou decrescente, sem que essa afirmação possa ser despropositada a qualquer momento, considerando o quão devastador poderá ser um atentado só. Ou seja, tendo em conta o número reduzido de mortes ou feridos ocorridos no RU ou nos EUA, em termos médios (comparando com outros países mais fustigados), um só ataque é capaz de incrementar de modo exponencial os valores desses registos, como foi o exemplo do “11 de Setembro” no EUA ou o “7 de Julho” no RU. Logo, poder-se-á afirmar que a tendência da ameaça terrorista (em termos de mortes e feridos) no RU e nos EUA é inconclusiva em função da amostra insuficiente.

2.3. A ABORDAGEM DO CONTRATERRORISMO

“O contra-terrorismo compreende um conjunto de atividades e de políticas integradas que visam combater o terrorismo e a ameaça terrorista” (Lara, 2007, p. 57). O Concelho da UE (2019), no plano regional, define-o como a estratégia que visa proteger os cidadãos e as infraestruturas e reduzir a vulnerabilidade a atentados, limitar a capacidade de planeamento e organização dos terroristas e encaminhar esses terroristas a tribunal, preparar, gerir e minimizar as consequências de um atentado terrorista e cooperar internacionalmente em matéria de luta contra o terrorismo.

No plano metodológico, a ação contraterrorista poderá ser adotada por duas vias, a *defensiva* e a *ofensiva*. A *defensiva*, também designada por antiterrorismo, funda-se essencialmente na atuação a jusante do ato terrorista, exercendo ações de preempção ou reação, geralmente postas em prática após o insucesso de uma ação *ofensiva*. A ação *ofensiva* (contraterrorista propriamente dita) compreende o conjunto de medidas destinadas a combater o fenómeno a montante da ação terrorista (Matos H. J., 2018, pp. 252-253). A vertente *defensiva* compreenderá medidas como a segurança de fronteiras, a implementação de sistemas de vigilância tecnológica, a aplicação de medidas de exceção temporárias, a implementação de sistemas de alerta precoce, o aumento de visibilidade no reforço das ações policiais, entre outras (Matos H. J., 2018, p. 252).

A vertente *ofensiva*, que foi abordada em pormenor no terceiro capítulo deste trabalho, representa uma ação proativa junto dos envolvidos na ação terrorista, com o recurso à inteligência, na pesquisa e recolha de informações sobre as suas capacidades e vulnerabilidades, penetrando nas suas estruturas através da infiltração ou do recrutamento de “agentes” (Matos H. J., 2018, p. 220). A inteligência, designadamente os serviços que desenvolvem esta atividade, também deverão, segundo Ribeiro (2016, p. 2016), ter um papel defensivo, nomeadamente apoiando as entidades a gerir as consequências de eventuais ataques de que tenham sido alvo e providenciando aconselhamento a essas na área da proteção.

Relativamente às medidas preventivas de combate ao terrorismo, estas deverão fundar-se na redução das vulnerabilidades existentes (produzindo uma avaliação de risco rigorosa dos cenários mais prováveis), na prevenção de potenciais incidentes (desenvolvendo capacidades na área da inteligência e da cooperação internacional), respondendo com prontidão (existindo incidentes, contendo e limitando as suas consequências) e investigando, identificando e punindo os seus autores (Fernandes L. F., 2004, p. 480).^{37 38}

Resumidamente, a resposta de um Estado (e da comunidade internacional) ao fenómeno terrorista, deverá ser o resultado de ações múltiplas e convergentes, cujo carácter preventivo, proativo e reativo visarão a prevenção, resposta, contenção e mitigação dos seus efeitos” (Matos H. J., 2018, p. 219) De forma paralela, mas inevitavelmente intrínseca ao fenómeno do terrorismo, deverá ser combatida a criminalidade organizada transnacional, dada a sua estreita ligação, procurando anular o financiamento providenciado por essa criminalidade às organizações terroristas (Lara, 2007, p. 65).

³⁷ Num plano estratégico, de intervenção em profundidade, Green e Protctor (2016, p. 28) apresentam como medidas preventivas contraterroristas o fortalecimento da resistência às ideologias extremistas, o investimento na prevenção orientada para a comunidade, a mobilização dos vários atores globais para cooperação no combate ao extremismo, o alinhamento das políticas e valores (zelando pelo cumprimento da lei e dos direitos humanos) e o desenvolvimento dos instrumentos de reação das forças militares e de segurança.

³⁸ Também Evans (2006, pp. 155-158), no plano estratégico, apresenta uma lista de objetivos por esta designados de “five P’s”: *estratégia de proteção*, envolvendo medidas antiterroristas, como por exemplo a proteção de fronteiras e espaço aéreo; *estratégia de policiamento*, potenciando as capacidades analíticas e reativas dos serviços de inteligência e das FSSD; *estratégia política*, alterando a atmosfera das comunidades problemáticas onde potenciais terroristas poderão, com maior probabilidade surgir; *estratégia de pacificação*, desenvolvimento económico e proteção dos direitos humanos, prevenindo o surgimento de novos conflitos; *estratégia psicológica*, procurando a alteração de mentalidades, mudando a forma como os cidadãos percebem e sentem o terrorismo, anulando qualquer vestígio de zona de conforto que alguns indivíduos poderão sentir, em roda do terrorismo

“Uma política de contraterrorismo, para ser efetiva, tem de ter natureza multidisciplinar, e só com uma avaliação da ameaça e do risco permitirá a redução do fator *P*” (Fernandes L. F., 2004, p. 481). Essa avaliação só poderá ter resultados se houver “articulação no seio da comunidade de informações, sendo fundamental o cruzamento rápido de dados, visando, depois do seu tratamento, a difusão pelas forças de segurança, num permanente ciclo de produção de informações” (Romana, 2004, p. 262).

3. A HUMAN INTELLIGENCE NO CONTRATERRORISMO ANGLO-AMERICANO

3.1. METODOLOGIA DA HUMAN INTELLIGENCE

A HUMINT, tradicionalmente conhecida por espionagem, é o conjunto de dados e informações, recolhidos a partir de fontes abertas ou classificadas, recorrendo à constatação dos comportamentos, eventos ou objetos (Fernandes L. F., 2014, p. 111). Joseph Wippl (2016, p. 586) define HUMINT, por um lado, como os agentes que fornecem informações secretas que permitem compreender os eventos ocorridos, auxiliando na tomada de decisão política, e por outro, como os agentes que influenciam a ocorrência de eventos para promover uma agenda de um governo. Este caracteriza a espionagem como uma atividade passiva/ativa, onde o agente define também o curso dos acontecimentos, não se limitando a observá-los.

A ação encoberta, subjacente à HUMINT, requer a dissimulação de identidade por parte de um agente, recolhendo assim informações de determinada organização (infiltração) ou a obtenção dessa através de um membro dessa organização (penetração, ou recrutamento), constituindo essa ação, segundo Pereira (2005, p. 36), um meio imprescindível na produção de inteligência. Quanto à dissimulação, de modo a que um operacional de inteligência consiga o acesso e assim recolher informações de locais e pessoas, que de outra forma não seria bem-sucedido, este poderá dissimular a sua identidade, utilizando uma “cobertura” adequada ao contexto, ocultando a parte real que poderia ser um entrave aos seus intentos. Uma vez obtido o acesso, iniciar-se-ão as operações de pesquisa de informações, por si mesmo ou através do recrutamento de outras pessoas, socorrendo-se de algum tipo de “manobra” que assegure a cooperação do recrutado. Esta “manobra” recairá muitas vezes na manipulação ou no suborno, chegando, se necessário, a recair na intimidação ou na coerção hostil (como por exemplo, a chantagem) (Bellaby, 2017, p. 399).

Assume-se assim que a HUMINT se fragmenta em dois métodos primordiais de pesquisa: a *infiltração* e a *penetração*. A *infiltração*, enquanto procedimento de obtenção encoberta de informações, visa preparar um ser humano para entrar num ambiente de grupo, claramente hostil, tendencialmente criminoso, e nele permanecer, simulando sustentadamente uma identidade fictícia. Esta ação deverá ser desenvolvida por um agente do organismo com

necessidade de conhecer (de força de segurança, militar ou de serviço de inteligência), mas também através de um agente externo a este. Este, no plano de produção de inteligência contraterrorista, é o método mais arriscado e complexo de pesquisa de informações (Gómez, 2007, p. 1).

A *penetração*, contrariamente à metodologia anterior, é conseguida quando um elemento que já pertence à estrutura organizativa desse alvo, ou que 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 ação, na *penetração*, é feita de dentro para fora (Matos H., 2012, p. 12). Esta inicia com identificação de indivíduos que tenham acesso a informações desejáveis, ganhando a sua confiança, acedendo às suas vulnerabilidades e percecionando a suscetibilidade de ser recrutado. Posteriormente, desenvolvendo a relação, é proposta a colaboração, no que à partilha de informações diz respeito, existindo normalmente uma motivação monetária, de vingança ou outra, por parte da fonte recrutada, iniciando-se o fluxo informacional (Lowenthal, 2003, p. 74).

Outras tipologias de HUMINT são utilizadas também, nomeadamente com alguma preponderância no contexto atual de contraterrorismo, como são as *ligações*, a *monitorização*, as *vigilâncias* ou as *aquisições clandestinas*. Estas técnicas poderão ser ignoradas de eventuais, e sequenciais, *infiltrações* ou *penetrações*. As *ligações* visam o estabelecimento de contactos, mais ou menos formais, com organizações que possam ter conhecimento privilegiado sobre determinado fenómeno, podendo estar sediadas nos espaços geográficos onde os alvos atuam, como serão exemplo as embaixadas, as forças militares, de segurança, serviços de inteligência locais e as organizações não governamentais (ONG). Estas *ligações* têm representado um papel vital na missão de contraterrorismo contemporâneo, designadamente face ao terrorismo de matriz islâmica, dado a dispersão geográfica de organizações como a *Al-Qaida*, impossibilitando que um só serviço de inteligência tenha capacidade para abranger essa fragmentação (Byman, 2013, p. 13).

A *monitorização*, por sua vez, consiste no ato preliminar de observar as atividades de um indivíduo ou organização (num curto prazo) com o intuito de recolher informações relevantes que levem a uma operação posterior. A *vigilância*, já de um modo mais contínuo ou prolongado, visa observar esse indivíduo ou esse grupo, de forma clandestina, com vista a

recolher mais elementos que possam conduzir a outro tipo de operações (Mayer, 2016, p. 3). A *vigilância* poder-se-á considerar a segunda fase da *monitorização*. No que diz respeito às *aquisições clandestinas*, estas visam a captura de elementos físicos, detetores de elementos informacionais de forma não consentida, por parte do seu legítimo titular, recorrendo muitas vezes à fusão com outras disciplinas da fase da *pesquisa*, nomeadamente a TECHINT (Central Intelligence Agency, 2020). Serão exemplos dessas *aquisições* a filmagem, fotografia, apreensão de objetos ou documentos³⁹.

Paralelamente aos métodos de pesquisa HUMINT, seja por *infiltração*, *penetração* ou outros anteriormente descritos, importa conhecer outra destriça regularmente efetuada, no que à ação das FSSD diz respeito. Estas formas de atuação dividem-se em *ações encobertas* ou *ações clandestinas*. Conceptualmente poderão existir algumas discórdias entre estas tipologias, nomeadamente após consideração do espaço geográfico em causa⁴⁰.

As *ações encobertas*, segundo o United States Code (Office of the Law and Revision Counsel, 2020), no contexto norte-americano, são aquelas onde o governo dos EUA visa influenciar as condições políticas, económicas ou militares externas, onde o papel dos EUA não deverá ser reconhecido publicamente. DeVine (2019, p. 4) esclarece que esta visará influenciar os acontecimentos externos, enquanto alternativa à escalada militar, e, contrariamente à tradicional recolha de informações, não deverá ser passiva. Procurará desenvolver-se de forma dissimulada, pois, caso não fosse, seria contraproduativa para o papel e reputação dos EUA no resto do mundo.⁴¹

As *ações clandestinas*, à margem da lei, também no contexto norte-americano, são operações patrocinadas ou conduzidas de forma a manter o sigilo ou a ocultação, podendo incluir a

³⁹ Apreensão de documentos também designada de “DocEx” (*document exploitation*). Técnica menos preponderante, hodiernamente, considerando que organizações terroristas, como a *Al Qaida*, evitam o excesso de registo de atividades, procurando desburocratizar a sua ação, condicionando, assim, a recolha de informações pela via documental (Byman, 2013, p. 9).

⁴⁰ De salientar que o termo ação encoberta (*covert action*, concretamente) será uma criação norte americana, não sendo usada no vocabulário de outros serviços de inteligência (Shulsky & Schmitt, 2002, p. 76).

⁴¹ No que diz respeito às tipologias de ações encobertas Shulsky & Schmitt (2002, pp. 77-90) distinguem entre ações de apoio encoberto de um governo aliado, ações de influência de perceções de um governo estrangeiro (através de agentes de influência e do uso da informação e desinformação), ações de influência de perceções de uma sociedade estrangeira (também através dos agentes de influência e da propaganda anónima), ações de suporte a uma força política estrangeira aliada e de ações de influência de eventos políticos por meios violentos (mediante a utilização de forças paramilitares ou de atos específicos de violência ou destruição, incluindo os assassinatos).

recolha de informações (DeVine, 2019, p. 5). Graça (2010), esclarece que “operações clandestinas são as que envolvem um maior grau de secretismo, concretamente porque são planeadas à margem do direito internacional e dos países-alvo, e, tradicionalmente, podem servir para derrubar governos e levar a cabo raptos e assassinatos”. Contrariamente às *ações encobertas*, as *ações clandestinas* não necessitam de autorização presidencial, mas somente uma notificação ao congresso. (DeVine, 2019, p. 5).

3.2. O PANORAMA ESTRUTURAL DOS SERVIÇOS DE INTELIGÊNCIA NO EIXO ANGLO-AMERICANO

Em termos orgânicos, tanto nos EUA como no RU, verifica-se a existência de uma vasta rede de organismos produtores de inteligência, sejam elas de cariz securitário ou com outros fins estratégicos ou táticos, no âmbito de prossecução dos fins de cada Estado. Abordou-se, neste trabalho, as estruturas de inteligência, das duas distintas nações, ao nível macro (transversalmente competentes, em cada uma das nações), não elencando algumas outras agências, forças ou serviços que, em certa medida, também são produtores de inteligência securitária, mas a um nível mais local ou menos preponderante. São exemplos disso algumas forças de segurança, como a londrina *Metropolitan Police* ou a *New York Police Department*, que também desenvolvem a sua atividade de inteligência contraterrorista nas suas áreas de atuação circunscritas, ou seja, apesar de não estarem integradas nas “comunidades de inteligência” nacionais, também são parte ativa no esforço coletivo dessas comunidades.

3.2.1. ESTRUTURA DA INTELIGÊNCIA NOS EUA

Nos EUA verifica-se a existência de uma panóplia de organismos governamentais que colaboram para a produção de inteligência. Esse conjunto é designado de *Intelligence Community* (IC)⁴². A IC, segundo o próprio *website*, tem por missão recolher, analisar e distribuir inteligência externa e informações de contrainteligência para os líderes norte-

⁴² A IC é coordenada pelo *Director of National Intelligence*, tendo como incumbências, entre outras, a gestão orçamental e a produção do *briefing* diário de inteligência ao presidente do Estados Unidos da América (Graça, 2010, p. 263). Segundo o *website* do *Office of Director of National Intelligence*, gabinete do *Director of National Intelligence*, a sua missão central, para além das mencionadas anteriormente, é a coordenação e integração de inteligência produzida pelos membros que compõem a IC, estando na sua dependência três centros nacionais de inteligência, o *National Counterproliferation Center*, o *National Counterintelligence and Security Center* e o *National Counterterrorism Center* (Office of the Director of National Intelligence, 2019).

americanos de modo a que estes possam tomar decisões que salvaguardem os EUA, incluindo, enquanto consumidores, o presidente norte-americano, políticos, forças de segurança e forças armadas (Intelligence Community, 2020). Esta é uma federação de agências e organizações norte-americanas que trabalham separadamente, mas também de forma conjunta, conduzindo as atividades de inteligência necessárias à prossecução das relações externas e à proteção da segurança nacional dos EUA (ITTACG, 2009, p. 8).⁴³

A IC integra serviços de inteligência (que desenvolvem essa atividade exclusivamente), forças e serviços de segurança, forças militares e também órgãos que se encontram tendencialmente no plano governativo. Integram assim a IC, e alfabeticamente ordenados, a *Air Force Intelligence*, *Army Intelligence*, *Central Intelligence Agency* (CIA), *Coast Guard* (USCG), *Defense Intelligence Agency* (DIA), *Department of Energy – Office of Intelligence*, *Department of Homeland Security – Office of Intelligence and Analysis*, *Department of State Bureau of Intelligence and Research* (IRN), *Department of Treasury – Treasury Office of Terrorism and Financial Intelligence*, *Office of Director of National Intelligence*, *Drug Enforcement Administration – Office of National Security Intelligence*, *Federal Bureau of Investigation – National Security Branch* (FBI), *Marine Corps Intelligence*, *National Geospatial-Intelligence Agency*, *National Reconnaissance Office*, *National Security Agency* (NSA) e a *Naval Intelligence* (ITTACG, 2009, p. 9).

Organicamente, as agências/forças dependem de distintos setores do poder executivo, sendo que a grande maioria se subordina a secretarias específicas (dependendo da área de ação). A título de exemplo, a NSA depende da *Secretary of Defense*, o INR da *Secretary of State* e o FBI da *Attorney General*. Em regime de exceção, a CIA responde ao presidente dos EUA, por intermédio do *National Security Council*, sem se encontrar na dependência administrativa de uma secretaria específica. A CIA não produz inteligência para outros consumidores que não o maior decisor estratégico, o presidente norte-americano (Lowenthal, 2003, p. 25).

Em termos da missão de cada um dos serviços norte-americanos elencados, todos estes encaram a pesquisa e produção de inteligência como uma das suas incumbências funcionais,

⁴³ Segundo a Estratégia Nacional de Inteligência norte-americana, é um dos objetivos de missão o contraterrorismo, identificando, compreendendo e dissolvendo atores estaduais e não estaduais envolvidos no terrorismo e atividades correlacionadas, anulando as ameaças aos EUA, às suas pessoas, interesses e parceiros (Office of the Director of National Intelligence, 2019, p. 12).

sendo que alguns se dedicam em regime de exclusividade à produção de inteligência (a CIA, por exemplo), enquanto outros têm um *core business* díspar, apesar também se dedicarem paralelamente à problemática da inteligência (a USCG, a título exemplificativo).

Os serviços que dependem da *Secretary of Defense*, naturalmente, produzem inteligência de cariz mais militar e tático, sendo que fornecem conteúdo de cariz estratégico ao poder executivo. A NSA é a organização criptográfica com a incumbência de proteger os sistemas de informação norte americanos e, cumulativamente, produzir inteligência a partir de sinais estrangeiros. É o serviço norte-americano que trabalha em exclusividade na SIGINT. A NGA é a agência de inteligência geoespacial que colabora essencialmente na aplicação operacional das forças militar norte-americanas, sendo o serviço de GEOINT com maior preponderância. A DIA é uma agência produtora de inteligência militar estrangeira, fornecendo ao decisor político inteligência sobre combatentes, políticas de defesa e estratégia estrangeiras, apoiando cumulativamente o planeamento e emprego das forças militares norte-americanas (Office of the Director of National Intelligence, 2020).

Ainda na dependência da *Secretary of Defense*, as convencionais forças armadas *Air Force Intelligence*, *Army Intelligence*, *Marine Corps Intelligence* e a *Navy Intelligence*, na área de inteligência, tem por missão providenciar inteligência extraída de meios aéreos, terrestres e marítimos, decorrente das missões específicas de cada uma das forças, recorrendo a ações de GEOINT, SIGINT, IMINT, MASINT, HUMINT e de contrainteligência. Nestas forças militares, a tendência é a produção de inteligência de cariz tático (Office of the Director of National Intelligence, 2020). Como se poderá constatar, uma significativa parte do esforço de produção de inteligência é desenvolvido por organismos integrados no *Secretary of Defense*.

Relativamente aos outros serviços, com a exceção da CIA, na dependência das respetivas secretarias, têm por missão a produção de inteligência nas suas áreas específicas de competência. O DoE é responsável pelas atividades de inteligência e contrainteligência, protegendo informações e tecnologias vitais para a segurança nacional, em matéria de segurança energética, fornecendo, cumulativamente, conhecimento técnico e científico ao poder executivo. O DoT recebe, analisa, agrupa e dissemina inteligência, desenvolvendo também ações de contrainteligência, estando ambas correlacionadas com as responsabilidades daquele departamento, detetando o financiamento de ações terroristas, da proliferação de

armas de destruição massiva, branqueamento de capitais, entre outras que ameacem a segurança nacional (Office of the Director of National Intelligence, 2020).

O FBI, enquanto serviço de segurança associado à justiça, no campo da inteligência é responsável por detetar as ameaças à segurança nacional num plano interno (desde o terrorismo, às armas de destruição massiva), garantindo também a vertente de contraespionagem norte-americana (Federal Bureau of Investigation, 2020). O INR, por sua vez, ocupa-se dos assuntos externos (diplomáticos) norte-americanos, recorrendo à pesquisa de distintas fontes, permitindo a reação atempada a mudanças de prioridades políticas estrangeiras, analisando e alertando precocemente os eventos e tendências externas que possam afetar a política externa norte-americana (Office of the Director of National Intelligence, 2020).

A CIA, produtora de inteligência para o *National Security Council*, por outro lado, incumbem-se da prevenção de ameaças e promoção dos objetivos de segurança norte-americana pela via da produção de inteligência recolhida de díspares fontes, recorrendo primordialmente às ações encobertas (Central Intelligence Agency, 2020). Esta agência ocupa-se, essencialmente, da vertente externa da produção de inteligência, mas também com incumbências de contra-inteligência, à semelhança do FBI, recorrendo, em termos de pesquisa, essencialmente à HUMINT, a GEOINT, COMINT e à OSINT (Pringle, 2019).

3.2.2. ESTRUTURA DA INTELIGÊNCIA NO REINO UNIDO

No que diz respeito à comunidade de inteligência no RU, é também esta composta por vários organismos (em quantidade não tão substancial como a norte-americana), sendo fiscalizada pela *Intelligence and Security Committee*⁴⁴. Integram esta comunidade as agências de inteligência *Government Communications Headquarters* (GCHQ), *Security Service* (MI5) e o

⁴⁴ Esta comissão é formada por 9 deputados selecionados pela Câmara dos Lordes e pela Câmara dos Comuns, sendo nomeados pelo Primeiro Ministro para examinar a política, administração e gastos das agências de inteligência e segurança (Gov.uk, Intelligence and Security Committee, 2020).

*Secret Intelligence Service (SIS)*⁴⁵. Integram, também, quatro organismos governamentais, não designados por “agências”, como as três anteriores, o *Defence Intelligence (DI)*, o *Office for Security and Counter-Terrorism (OSCT)*, o *Joint Intelligence Organization (JIO)* e o *National Security Secretariat (NSS)* (Intelligence and Security Committee of Parliament, 2018, p. 3).

Em termos orgânicos, o MI5 depende da *Home Secretary*. o SIS e o GCHQ da *Foreign Secretary* e o DI do *Defense Secretary* (as secretarias dependem diretamente do primeiro ministro britânico). O JIO responde diretamente ao primeiro ministro, sem estar sob a alçada de qualquer secretaria (Matos H. J., 2018, p. 137). O NSS também não se encontra na dependência de uma secretaria, sendo que foi constituído para dar apoio ao *National Security Council*⁴⁶ (Gov.uk, 2020). O OSCT está na dependência do *Home Office* (departamento ministerial) (Gov.uk, 2020).

No que diz respeito à missão das agências e organismos de inteligência no RU, o GCHQ trabalha, essencialmente, na pesquisa de informações pela via da COMINT, alimentando os restantes serviços, o MI5 foca-se na segurança interna do RU, recolhendo e analisando informações conducentes a esse objetivo (recorrendo a vários métodos de pesquisa) e o SIS, numa vertente global, visa desenvolver contactos externos e recolher informações de cariz contraterrorista e outras associadas aos conflitos internacionais (socorrendo-se também de dispareas formas de pesquisa). O DI recolhe e analisa inteligência para a suas forças armadas, assim como, inteligência intrínseca à segurança nacional, o NSS coordena os assuntos governamentais de segurança e inteligência, o OSCT providencia a coordenação necessária para um estratégia contraterrorista do RU, e o JIO apoia o *Joint Intelligence Committee*, que compõe os altos funcionários dos ramos da inteligência e da política, produzindo avaliações de inteligência para o poder executivo (Intelligence and Security Committee of Parliament, 2018, p. 3).

⁴⁵ Também usualmente designado por MI6.

⁴⁶ Fórum para discussão governamental dos objetivos do governo para segurança nacional.

3.3. PRÁTICAS NORTE-AMERICANAS

3.3.1. ARMY INTELLIGENCE

Um dos manuais norte-americanos que retrata o *modus operandi* em matéria de HUMINT é o FM 2-22.3– Human Intelligence Collector Operations (2006). Este manual militar, produzido pelo Departamento do Exército norte-americano, apesar de não se debruçar em específico na temática do contraterrorismo, optando por uma abordagem procedimental mais generalizada, sugere a sua utilização nesse campo. Considerando a sua data de publicação, após o 11 de setembro de 2001, é este, inevitavelmente, um manual de práticas contraterroristas, dado o enfoque norte-americano a partir dessa data, quer no plano da segurança, como no plano da defesa. A frequente menção ao tema terrorismo no texto do manual é espelho disso mesmo. Este foca-se, essencialmente, na prática da pesquisa HUMINT onde a fonte não está sob custódia das forças militares, contrariamente ao documento trabalhado no ponto seguinte, o Report RL32567 (2004) do Department of Defense (DoD). Não aborda métodos de infiltração, mas sim de penetração (recrutamento), nos grupos/organizações antagónicas à força que aplica as práticas.

O manual operativo está dividido em quatro partes: Apoio, Planeamento e Gestão da HUMINT; Pesquisa HUMINT em Operações Militares; O Processo de Pesquisa HUMINT; Análise e Ferramentas. A primeira parte aborda, de forma introdutória, o papel da HUMINT no apoio a operações militares assim como outros aspetos de relevo em matéria de gestão das operações, nomeadamente de comando e supervisão destas. A segunda, que foi abordada em pormenor, vem definir os tipos de operações HUMINT, nomeadamente as operações de *contacto*, as de *debriefing*, as de *ligação* e as de *interrogatório*.

As operações de *contacto* são aquelas onde se busca o contacto entre o operacional de pesquisa HUMINT, que visam a recolha de informações (pela via de díspares técnicas de pesquisa HUMINT), e a fonte humana, que poderá ser convencida a divulgar informações. Segundo o manual, existem três tipos de contactos: os *singulares*, os *contínuos* e os *formais*. Os *singulares*, como o próprio nome indica, ocorrem somente uma vez, podendo surgir de patrulhas, detenções ou de *checkpoints* de controlo. Deverão ser contactos básicos, com vista à obtenção de informações básicas, como o nome, morada ou outro elemento identificativo,

carecendo este, no entanto, de corroboração de outras fontes. Aqui, o operacional de pesquisa, com base nos elementos básicos recolhidos, deverá procurar entender se o contacto singular poderá converter-se num contínuo (p. 78). Os contactos *contínuos* serão aqueles com maior potencial do que os anteriores, sendo passíveis de permitir a extração mais avolumada de informações. Estes, deverão providenciar informações de uma forma sistemática, mas informal, pela via do *debriefing* e da elicitação⁴⁷. Os contactos *formais* são aqueles que, de forma consciente, se propõem a facultar informações aos operacionais, sabendo que são alvo de uma ação de pesquisa HUMINT (p. 82).

As operações de *debriefing* são aquelas que se referem à inquirição sistemática de indivíduos, que não estão na custódia das forças militares norte-americanas, com vista à recolha de informações, com recurso a técnicas diretas ou indiretas de interrogatório. As operações de *debriefing* poderão ser de nível tático, inquirindo civis que possam esclarecer pormenores relevantes às operações em curso, em campos de refugiados ou a forças militares aliadas. Estas são excelentes fontes de informação, pelo contacto que vão tendo com as populações e com o ambiente) e operações de *debriefing* estratégico (p. 84).

As operações de *ligação*, por sua vez, visam a obtenção de informações e assistência, desenvolvendo visões comuns com os pares, sendo as fontes normalmente membros governamentais, militares, forças de segurança, entre outros cidadãos locais. Procuram estabelecer relações de trabalho com outros organismos, trocando inteligência operacional, facilitando o acesso a registos de outros organismos, que de outra forma não seriam adquiríveis. Por outro lado, as operações de *interrogatório* consubstanciam o processo sistemático de utilização de métodos de interrogatório a pessoas capturadas ou detidas, atendendo a pressupostos legais limitadores (elencados exaustivamente no manual), sob supervisão hierárquica. (pp. 88-89).

Relativamente à terceira parte do manual, que diz respeito ao processo de pesquisa HUMINT, este desfragmenta-o em cinco fases: a *triagem*, a *preparação e planeamento*, *aproximação*, *questionário* e o *relatório*. A fase da *triagem* é definida como aquela em que as fontes humanas são avaliadas e selecionadas, com base nos requisitos provenientes da fase anterior

⁴⁷ Os típicos de contactos contínuos são os trabalhadores locais, trabalhadores deslocados, refugiados, oficiais de ligação ou detidos (pp. 80-82).

do ciclo de produção de inteligência, o *planeamento*. Haverá uma categorização e priorização das fontes, com base na probabilidade de uma dessas estar na posse de informações prioritárias, atendendo também ao nível de cooperação expectável da fonte⁴⁸.

A *triagem* procurará avaliar um indivíduo ou um grupo de indivíduos, determinando o seu potencial para dar resposta aos requisitos de pesquisa, identificando as pessoas que poderão encaixar-se no perfil (predeterminado) de fonte. Esta avaliação, deverá desenvolver critérios que serão definidos como indicadores de informação potencial, não desconsiderando aspetos como o grupo étnico, o género, a aparência ou o estatuto social. Em suma, na *triagem*, deverão ser identificados os indivíduos, entre o grupo alvo, que poderão ter informações potencialmente valiosas e que, cumulativamente, estejam dispostos ou possam ser persuadidos a cooperar⁴⁹ (pp. 117-118).

Na segunda fase, a *preparação e planeamento*, segundo o manual, o recolector de informações HUMINT deverá manter em mente o objetivo determinado, satisfazendo os requisitos predefinidos, contribuindo para a missão incumbida. O objetivo da pesquisa deverá ser previamente planeado e preparado. A subfase da *preparação* deverá incluir a prévia organização de tarefas, o ponto de situação (relativamente às vulnerabilidades/potencialidades atuais do opositor), o esclarecimento dos objetivos inerentes à missão, os eventos atuais no local de atuação (que poderão influir na intervenção), os requisitos específicos de pesquisa, a análise de manuais ilustrativos do cenário onde ocorrerá a operação (em termos geográficos) e ainda as conclusões extraídas de relatórios de HUMINT anteriores (pp. 127-128).⁵⁰

⁴⁸ Segundo o manual, este processo requer indivíduos com experiência, maturidade e capacidade de julgamento, sendo estes plenamente conhecedores dos requisitos de pesquisa, estando assim capacitados para tomarem decisões com base em informações limitadas (p. 110).

⁴⁹ Nesta dupla averiguação, do nível de conhecimento e do nível de cooperação, o manual analisado determina a utilização de uma tabela, onde, em termos de conhecimento, os níveis oscilam entre A e C (A – Provavelmente detém informações prioritárias; B – Poderá deter informações prioritárias; C – Não aparenta deter informações de relevo) e, em termos de cooperação, oscilam entre o grau 1 e 3 (1 – Responde às questões diretamente; 2 – Responde de forma hesitante à inquirição; 3 - Não responde à inquirição). A conjugação entre o nível de conhecimento e o nível de cooperação, definirá a prioridade de abordagem, sendo a conjugação de níveis 1-A a mais credível, onde essas fontes deverão ser questionadas de forma prioritária, contrariamente a uma fonte de nível 3-C, que não deverá ser sequer considerada (p. 118).

⁵⁰ Ainda na subfase da preparação deverá haver uma pesquisa específica à fonte a abordar (tarefa designada de *vetting*). Essa pesquisa poderá fornecer pistas sobre o conteúdo informacional que a fonte poderá possuir e que técnicas de abordagem (terceira fase) deverão ser aplicadas. Interessará conhecer a área geográfica associada à fonte (denunciando fatores como a etnia, por exemplo), as línguas faladas pelo alvo, a afiliação política e

Relativamente à segunda subfase, do *planeamento*, após a pesquisa preparativa, deverá ser desenvolvido um plano de abordagem à potencial fonte, idealmente com um apoio de um analista⁵¹. Aqui, o plano deverá conter, uma vez mais, os requisitos de pesquisa HUMINT, a localização e o momento temporal para a abordagem de inquirição, o modelo de abordagem primário e o alternativo, o plano de questões a efetuar (incluindo tópicos a serem contemplados e a sequência destes) e o método de gravação e de relato dos dados informativos obtidos (pp. 132-133).

Seguidamente, na fase da *abordagem*, dever-se-á salientar que, independentemente do tipo de operação, a primeira impressão causada pelo operacional de pesquisa HUMINT à fonte e a abordagem que o primeiro adota para obter a cooperação do segundo, terá um efeito duradouro no relacionamento entre ambos e no grau de sucesso da recolha de informações almejada. A tipologia de abordagem deverá variar consoante as características da operação, o ambiente operacional, o estatuto social da fonte, a personalidade desta, do tipo de personalidade e experiência do próprio operacional de pesquisa e do tempo disponível para a operação. O sucesso da operação dependerá, em grande medida, do desenvolvimento da vontade inicial da fonte em comunicar. Os inquiridores deverão ter um entendimento profundo das especificidades culturais e emocionais da fonte, selecionando estratégias de abordagem conducente ao resultado pretendido (pp. 139-140).

O objetivo do operacional de pesquisa HUMINT, nesta fase, será estabelecer um relacionamento com a fonte, promovendo o fornecimento de informações precisas e confiáveis, em resposta às questões efetuadas. Deverá adotar uma *persona* apropriada à fonte (após a avaliação minuciosa), permanecendo alerta para quaisquer pistas, verbais ou não verbais, que possam indicar a necessidade de mudança de técnica de abordagem. O tempo despendido nesta terceira fase do processo de pesquisa HUMINT dependerá, essencialmente, do manancial de informações que a fonte possui, da disponibilidade de outras potenciais

religiosa, o nível de educação, o emprego, o estatuto social e eventual registo criminal (denunciador do comportamento, mais ou menos divergente, daquele) (p. 129).

⁵¹ Verifica-se aqui a apologia à fusão funcional entre os operacionais da fase da *pesquisa* e os da fase da *análise*, defendendo este manual a interdependência das fases, no que diz respeito ao ciclo de produção de inteligência, à semelhança do defendido por Heitor Romana. Segundo o autor, “é fundamental, no novo contexto da análise do fenómeno terrorista, a aposta na “análise operacional”, entendida como a integração e síntese de informações, utilizando os procedimentos próprios do *desk system*, mas a partir de indícios técnicos (*raw material*) obtidos e trabalhados diretamente no terreno de pesquisa. Esta opção metodológica permite uma maior rapidez de avaliação, ainda que tenha que ser alvo de uma monitorização da sua fiabilidade” (Romana, 2005, p. 4).

fontes com conhecimento sobre os mesmos tópicos e do tempo disponível (p. 140).

Segundo o manual, independentemente do tipo de fonte e da sua personalidade mais extrema, todas as fontes possuem características exploráveis, que, se forem devidamente detetadas pelo operacional de HUMINT, serão úteis na facilitação do processo de recolha. A deteção far-se-á pela via da fala, dos maneirismos, das expressões faciais ou mesmo de reações involuntárias, como a transpiração ou o movimento dos olhos. Face a estas exteriorizações, o recolector terá de adaptar casuisticamente a sua abordagem, sendo que, no entanto, existem ações comuns em todas as abordagens, que deverão ser atendidas pelo gestor da fonte. São exemplo disso, o estabelecimento e conservação do controlo sobre a fonte, o estabelecimento e controlo sobre o relacionamento criado e a necessidade de identificação das emoções primárias, valores, tradições e outras características que poderão ser exploradas para a manutenção da cooperação (p. 141). Sendo a confiança a base do relacionamento entre a fonte e o operacional de HUMINT, que se traduz na cooperação, a *persona* criada terá de ser realista, fazendo-se passar por outrem com uma posição social/hierárquica que se coadune com a idade, aparência e experiência profissional deste (p. 142).

Quanto às técnicas de *abordagem*, propriamente ditas, o manual elenca a *abordagem direta*, onde as questões pertinentes são efetuadas diretamente, a *abordagem de incentivo*, onde é concedida uma recompensa real ou emocional, e a *abordagem emocional*, onde se conjuga uma resposta emocional associada a um determinado incentivo (pp. 144-146)⁵².

Posteriormente, na fase do *questionário*, as questões deverão ser formuladas numa sequência lógica, evitando negligenciar tópicos relevantes, obtendo o conhecimento pertinente da fonte em cada pergunta, antes de avançar para a próxima. O inquiridor, deverá usar vocabulário claro, compreensível e que não seja ambíguo, adaptando o questionário ao nível intelectual do

⁵² A *abordagem emocional* subdivide-se na *abordagem de amor emocional*, *abordagem de ódio*, *abordagem de incremento de medo*, *abordagem de decréscimo de medo*, entre outras descritas (o manual, naturalmente, é exaustivo nas distintas tipologias de abordagem). Na *abordagem de amor emocional* apela-se à amizade, à camaradagem, ao patriotismo ou ao amor pela família, explorando a eventual ansiedade da fonte, associada a um desses fatores. Na *abordagem de ódio*, o operacional de HUMINT explora o ódio ou desejo por vingança da fonte (que, por exemplo, poderá estar correlacionado com sentimentos negativos demonstrados pela fonte em termos do regime político onde esta está inserido ou também pelo descontentamento com os superiores hierárquicos daquela). A *abordagem de incremento de medo* consiste na deteção de um dado medo preexistente da fonte, ou criação de um novo, explorando e, posteriormente, reduzindo-o, obtendo assim a cooperação da fonte. Na *abordagem de decréscimo de medo*, também existirá a deteção do medo preexistente, procurando minorá-lo verbalmente, acalmado a fonte, fazendo-a olhar para o recolector como um protetor, existindo assim maior cooperação (pp. 146-156).

inquirido. Se o inquirido possuir uma capacidade cognitiva significativa e o nível de conhecimento técnico for superior ao do inquiridor, então deverá existir uma preparação cuidada das questões a formular, com o apoio técnico ao operacional HUMINT, se necessário (p. 163). Relativamente aos tipos de questões, estas poderão *questões iniciais*, *questões de acompanhamento*, *questões não pertinentes*, *questões de repetição*, *questões de controlo* e *questões preparadas* (pp. 163-165). Dever-se-ão evitar *questões dirigidas*, *questões negativas*, *questões compostas* ou *questões vagas* (pp. 166-167).

Pormenorizando as tipologias elencadas, as *questões iniciais* visam perspetivar o decurso da inquirição, obtendo somente informações básicas sobre o tópico. As *questões de acompanhamento* são usadas para expandir e completar as informações obtidas nas questões iniciais. As *não pertinentes* não visam qualquer objetivo de pesquisa, mas sim consolidar o relacionamento entre o inquiridor e o inquirido. As *de repetição* visam confirmar a precisão e veracidade das informações obtidas anteriormente, da mesma fonte, analisando o grau de confiança desta (devendo ser formuladas diferentemente e em momentos díspares, para que a fonte não perceba que está a ser testada). As *de controlo* visam confrontar informações recolhidas anteriormente, de outras fontes, com a resposta atual do inquirido, percecionando, uma vez mais, a confiança e veracidade dos factos fornecidos pelo inquirido. As *preparadas*, como a própria nomenclatura indica, são aquelas que são previamente analisadas, sendo formuladas com precisão e detalhe, após trabalho de pesquisa analítica ou técnica (pp. 164-166).

Relativamente às questões que não deverão ser formuladas, as *questões dirigidas* são aquelas em que o inquirido responde de forma fechada, com “sim” ou “não” (por exemplo), proporcionando maior facilidade na mentira e protelando a inquirição. As *negativas* condicionam, por vezes, a compreensão do inquiridor, nomeadamente quando a pergunta é negativa e a resposta também é negativa, não sendo totalmente perceptível qual a orientação de resposta do inquirido, face à temática questionada. As *compostas*, que consistem em duas ou mais perguntas interligadas na mesma, permitem que o inquirido se consiga evadir a uma das partes que não lhe interesse responder ou que ocorra a confusão no inquirido, acabando por não satisfazer as necessidades informacionais. As *vagas*, por fim, poderão não facultar a informação suficiente para a compreensão da fonte, relativamente às necessidades do inquiridor (pp. 166-167).

As respostas às questões deverão ser registadas de modo preciso e íntegro, recorrendo às técnicas de gravação mais adequadas ao contexto, podendo o inquiridor socorrer-se da memória (a técnica que promoverá maior interatividade e menor grau de desconfiança na fonte), anotações escritas (ou digitadas) ou gravação em áudio e/ou vídeo. As vantagens e desvantagens de cada técnica deverão ser ponderadas casuisticamente (pp. 171-173).

A inquirição também poderá ocorrer pela via da elicitación, onde se obtêm informações por uma via da interação direta com a fonte, sendo que a fonte não está ciente do objetivo específico da conversa. Esta técnica, deverá ser usada quando outras formas convencionais de inquirição não resultem, devendo este ser um processo sistemático e planeado, requerendo uma preparação minuciosa (p. 167). O manual, ainda no âmbito da temática da inquirição, aborda o *engano*, enquanto provável manobra do inquirido. Esclarece que, apesar de as inconsistências nas ações ou palavras da fonte não indicarem necessariamente uma mentira, da mesma forma que a consistência não é condição *sine qua non* para a verdade, um padrão de inconsistências inexplicáveis normalmente representa um engano, requerendo elevada experiência do operacional de HUMINT para a sua deteção ⁵³ (p. 168).

No que diz respeito à última fase do processo de pesquisa em HUMINT, o *relatório*, as informações recolhidas deverão atender aos princípios de precisão, celeridade, clareza, coerência, integridade, oportunidade e disseminabilidade (p. 179). O manual FM 2-22.3 elenca dois tipos de relatório, de grosso modo, os *operacionais* e os de *gestão de fontes*. Os *operacionais* não contêm as informações recolhidas com o intuito de responder às necessidades de inteligência, nomeadamente aquelas que possam estar correlacionadas com os aspetos sensíveis inerentes à pesquisa HUMINT. Estes incluem essencialmente aspetos associados à logística e a questões administrativas, respondendo a necessidades paralelas à gestão de fontes (p. 180). Relativamente aos relatórios de *gestão de fontes*, estes poderão assumir a forma de *relatório de informações de inteligência*, *relatório 'SALUTE'*, *relatório de dados de fontes básicas*, *relatório de contacto*, entre uma panóplia de outros tipos de

⁵³ Como forma de deteção, dever-se-á recorrer às questões de repetição e de controlo, à análise da linguagem corporal, à perceção de inconsistências entre o nível de conhecimentos e o grau/nível hierárquico da fonte numa determinada organização (que por vezes é superior ou inferior ao nível que o inquirido afirma ter), à constatação da falta de detalhe de afirmações prestadas ou da ausência de vocabulário técnico (que a fonte deveria ter, considerando a personagem por vezes criada pela própria fonte), entre outras (p. 169). Como forma de desmascarar as inconsistências, o inquiridor deverá formular as questões de modo a requerer respostas pormenorizadas, alterar entre tópicos, usar o polígrafo, entre outras. Relativamente às inconsistências, deverá assinalá-las ao inquirido, pedindo a justificação das mesmas (p. 170).

relatórios, discriminados no manual ⁵⁴ (pp. 181-182).

A quarta parte do manual aborda a análise e produção HUMINT. Esta irá suportar o planeamento operacional, orientando as operações HUMINT. Os analistas determinam o grau de consistência das fontes, baseando-se em fatores como a localização e acesso à fonte ou informações anteriores sobre a fonte, determinando se estas são completas, verdadeiras e se existe adequação aos requisitos de pesquisa. Estes processos analíticos fornecerão informações de apoio à cadeia de comando. Segundo o manual FM 2-22.3, uma vez mais se afirma que a análise terá de ser parte integrante da pesquisa HUMINT, ocorrendo durante todo o processo, sendo dividida em quatro categorias: o *suporte analítico ao planeamento e direcionamento operacional*, *análise e avaliação operacional*, *análise da fonte* e a *análise e produção HUMINT* (enquanto disciplina única) (pp. 202-203).

3.3.2. DEPARTMENT OF DEFENSE (DOD)

Quanto ao DoD norte-americano, através do *website Wikileaks*, foi possível obter alguma documentação intimamente relacionada com a HUMINT no contraterrorismo, nomeadamente no que diz respeito às técnicas de interrogatório aplicadas às fontes humanas, em uso pelas forças militares daquele país. Uma vez mais, e à semelhança do manual anteriormente dissecado, as matérias aqui versadas dizem respeito à extração de informações pela via da penetração, recrutando de “dentro para fora”, sem infiltração de operacionais nas organizações⁵⁵. No entanto, o relatório que se segue, aborda a pesquisa HUMINT na vertente

⁵⁴ O *relatório de informações de inteligência* é usado para relatar todas as informações HUMINT recolhidas em resposta aos requisitos de pesquisa, sendo usado enquanto pormenorização dos factos reportados pelo relatório SALUTE. O *relatório 'SALUTE'* é aquele que visa reportar informações de interesse imediato para indivíduos de qualquer escalão, reportando informações relevantes às unidades que serão afetadas por aquele conjunto de informações, ou pela inexistência delas. O *relatório de dados de fontes básicas* providencia à cadeia de HUMINT os elementos biográficos e operacionais básicos, relacionados com a fonte trabalhada. O *relatório de contacto* é usado pelos operacionais de HUMINT (recolectores) para relatar à cadeia técnica informações relevantes, especificamente correlacionadas a um contacto com uma determinada fonte, em específico (p. 181).

⁵⁵ Considera-se que os interrogatórios de detidos poderão, em contexto de produção de inteligência, assumir-se como uma forma de penetração em organizações terroristas. Apesar de estarmos a falar de uma obtenção de informações forçada, sem consentimento da fonte “recrutada”, poder-se-á assumir enquanto metodologia HUMINT. Poderá, em contraposição, não ser visto como forma convencional de penetração de organizações antagónicas àquela que interroga, sendo, no entanto, um importante método, no que ao terrorismo de matriz islâmica diz respeito, independentemente da utilização, ou não, da tortura não legitimada (Byman, 2013, p. 8). O interrogatório de fontes detidas, poderá funcionar somente enquanto instrumento intermediário do recrutamento, ou seja, através da conversão de detido num agente duplo, servindo de “alavanca” para a penetração póstuma (O agente duplo espia uma «organização alvo» em benefício de uma outra organização, mas na verdade é leal ao «alvo» (Graça, 2010, p. 243)).

do interrogatório à fonte detida (sob custódia) pelas forças armadas, enquanto o manual FM 2-22.3 se foca nos questionários aplicados a fontes humanas que não estão, tendencialmente, detidas.

O Report RL32567 (2004), debruça-se sobre a “Legalidade das técnicas de interrogatório à luz da Convenção de Genebra⁵⁶”, elencando diversas metodologias de interrogatório utilizadas pelas forças armadas na dependência do DoD, sendo umas tacitamente aprovadas e outras pendentes de aprovação do comando militar (Elsea, 2004, p. 3). Este relatório surge após a divulgação de imagens veiculadas pela comunicação social, onde, alegadamente, militares do exército norte-americano torturavam prisioneiros iraquianos na prisão de Abu Ghraib. O relatório vem discutir e analisar as técnicas de interrogatório aprovadas e consideradas durante os interrogatórios de Abu Ghraib (2004, p. 5). Poder-se-á, a partir deste relatório, compreender quais as práticas de interrogatório admissíveis pelo estado norte-americano, não só à luz deste contexto específico, mas também noutros cenários de intervenção contraterrorista. O relatório ressalva que os métodos aprovados se aplicam a detidos suspeitos da prática de terrorismo, limitados pelas Convenções de Genebra e Haia (2004, p. 23).

Relativamente às técnicas de interrogatório aprovadas (sem autorização superior), que no FM 2-22.3 são designadas de técnicas de questionário⁵⁷, o relatório lista-as como a *direta, incentivo/retirada de incentivo, amor/ódio emocional, aterrorização severa/suave, redução de medo, potenciação/redução do orgulho & ego, futilidade, nós sabemos tudo, estabelece a tua identidade, repetição, ficheiro & dossier, disparo rápido e silêncio* (2004, pp. 23-31).

Na técnica *potenciação/redução do orgulho & ego*, no que diz respeito ao primeiro subtipo, a *potenciação do orgulho & ego*, procura-se induzir a fonte a revelar informações pertinentes através da bajulação, potenciando o ego e a confiança. Utiliza-se, essencialmente, em fontes que demonstrem sentir-se inferiores na cadeia organizacional onde estão inseridos, podendo assim ter a oportunidade de demonstrar o seu intelecto ou relevância, revelando informações

⁵⁶ “As Convenções de Genebra e seus Protocolos Adicionais são tratados internacionais que contêm as normas mais relevantes que limitam as *barbáries* da guerra. Elas protegem pessoas que não participam dos combates (civis, pessoal de saúde, profissionais humanitários) e as que deixaram de combater (militares feridos, enfermos e náufragos, prisioneiros de guerra)” (Comité Internacional da Cruz Vermelha, 2020).

⁵⁷ Parte destas técnicas foi abordada aquando da descrição do manual FM 2-22.3, na fase da *abordagem*, do processo de pesquisa em HUMINT, pelo que não serão novamente pormenorizadas.

que não se revelariam noutra circunstância. No que diz respeito ao segundo subtipo, a *redução do orgulho & ego* e, em contraste do anterior, visa-se denegrir a imagem que a fonte tem de si mesma, nomeadamente no que diz respeito às suas capacidades, competências técnicas, lealdade, qualidades de liderança ou outras fraquezas percecionadas pelo interrogador. Usando, o interrogador, um tom sarcástico, demonstrando desapontamento, poderá fazer com que a fonte fique na defensiva, tentando em seguida provar o seu valor e o quão errado está o interrogador, facultando assim as informações requeridas inconscientemente (pp. 33-34).

Através da técnica *futilidade*, são exploradas as dúvidas e apreensões preexistentes do interrogado, levando-o ao desespero, de modo a fazê-lo acreditar na inutilidade da tentativa de resistência ao interrogatório. O relatório admite que a técnica, levada ao extremo, poderá induzir sofrimento mental gravoso o suficiente para levantar questões sob as Convenções de Genebra (p. 30). A técnica *nós sabemos tudo* procura fazer com que a fonte acredite que o interrogador conhece todos os pormenores associados à mesma. Aqui, o interrogador faz perguntas para as quais já tem resposta e quando o interrogado se recusa a responder (ou responde com falsidade) o interrogador responde por ele, fazendo-o crer que conhece tudo sobre este (p. 34). Utilizando a técnica *estabelece a tua identidade* o interrogador insiste que a fonte foi identificada como um criminoso infame, que apenas se está a fazer passar por outra pessoa, para evitar as subjacentes punições. Ou seja, através da imputação de uma identidade forçada ao interrogado, a fonte poderá ser enganada e acabar por facultar informações pessoais detalhadas, para comprovar que não é a pessoa acusada (p. 34).

Na técnica *repetição* o interrogador repete várias vezes a mesma pergunta procurando que a fonte coopere. O tédio causado ao interrogado, pela repetição induzida, poderá levá-lo a dar respostas mais completas e sinceras, simplesmente para obter o alívio da monotonia. O relatório ressalva que esta metodologia, levada ao extremo, poderá causar o sofrimento psicológico (p. 34). A técnica *ficheiro & dossier* é uma variante da técnica *nós sabemos tudo*, onde é apresentado ao interrogado um conjunto de registos físicos com elementos informacionais subjacentes a este, acrescentando muito mais documentação em branco (fora do alcance visual do interrogado), criando a ilusão de que as informações detidas pelo interrogador são muito mais detalhadas do que são na realidade (pp. 34-35). Com a técnica *disparo rápido* um ou dois interrogadores formulam as questões a uma velocidade excessivamente rápida, impossibilitando a fonte de responder com coerência e consciência a

todas elas, conduzindo assim a contradições inevitáveis, que serão posteriormente exploradas pelos interrogadores (p. 35).

Por fim, na técnica *silêncio* o interrogador não diz nada, olhando somente para a fonte, diretamente nos olhos, preferencialmente com um leve sorriso no rosto, deixando o interrogado nervoso, forçando-o a quebrar o contacto visual. Este constrangimento poderá levar a própria fonte a começar a conversar ou fazer perguntas para quebrar a tensão. Seguidamente, quando o interrogador começar a fazer as perguntas, provavelmente o interrogado já estará mais aliviado e mais disposto a divulgar informações (p. 35).

Quanto aos métodos que, apesar de serem autorizados, terão de ser aprovados pelo “Comando General”⁵⁸, o manual elenca os seguintes: *mudança de cenário, manipulação alimentar, manipulação ambiental, ajuste do sono, isolamento, utilização de canídeos militares, privação sensorial, posições de stress, remoção de roupas, remoção de itens de conforto e barbear forçado* (p. 37). Serão agora pormenorizados.

Na técnica *mudança de cenário* o interrogador desloca o interrogado para um espaço físico menos confortável, afetando-o psicologicamente. Aqui, desde que não haja alteração nos níveis de saúde ou higiene, não violará a Convenção de Genebra, segundo o relatório (p. 36). No método da *manipulação alimentar* a dieta do interrogado será alterada, sem, no entanto, o privar de comida ou água, ou afetar a sua saúde, ou a sua convicção religiosa, procurando desorientar o interrogado, transtornando-o pela sua quebra de rotina (p. 36). Na técnica *manipulação ambiental* o interrogador irá alterar a temperatura da sala ou alterar o cheiro existente, onde se encontra o interrogado, sem, no entanto, ofender a integridade física do detido (pp. 36-37).

Na técnica *ajuste do sono*, o ciclo usual de sono do detido é alterado, revertendo-o, por exemplo, da noite para o dia, causando desorientação similar à causada pelo *jet leg*. A privação do sono, a existir, segundo o relatório, não deverá exceder os quatro dias (p. 37). Na técnica *isolamento*, o detido será isolado dos outros detidos, por períodos não superiores a 30 dias, com as condições de tratamento iguais aos restantes. O Report RL32567 define este

⁵⁸ Depreende-se que o manual se está a referir aos decisores estratégicos das forças armadas norte-americanas.

método com um de utilização excecional, não podendo atingir proporções de tortura ou tratamento cruel, desumano ou degradante (p. 38). Na técnica *utilização de canídeos militares*, são aproximados ao detido os cães, sem ameaça direta, criando ansiedade (mas não terror ou trauma), potenciando a probabilidade de colaboração da fonte (p. 38).

Por sua vez, na técnica *privação sensorial*, o interrogado é privado de imagens, sons, gostos, cheiros ou sensações táteis familiares, induzindo o stress (que, quando levado ao extremo, poderá causar alucinações ou delírios) (p. 39). Na técnica *posições de stress*, o detido é colocado numa posição (não definida em concreto pelo relatório) em permanência prolongada (também não descrita em termos de longevidade). O relatório assume que o uso de posições de stress poderá violar a Convenção de Genebra, por ser passível de induzir sofrimento ou humilhação, sendo que, no entanto, a extensão do sofrimento necessário para atravessar a linha estabelecida pela Convenção não esteja firmemente estabelecida (pp. 39-40). A técnica *remoção de roupas*, como a própria designação indica, visa despojar os detidos da sua identidade, apesar de se admitir que poderá colocar a saúde dos visados em risco. O intuito é criar um sentimento de desamparo e dependência, advertindo o relatório que deverá existir monitorização das condições ambientais, para que a técnica não prejudique a saúde do interrogado (p. 40).

A técnica *remoção dos itens de conforto*, visa a retirar de bens que possam traduzir bem-estar ao detido (como será exemplo um anel com simbolismo para o interrogado). O relatório aponta a Convenção de Genebra como ambígua neste aspeto, sendo que será possível a retirada de todos os objetos que não se encaixem na rúbrica *conforto*. Exclui liminarmente a retirada dos objetos religiosos, por considerar que viola a Convenção (p. 40). Por fim, o método *barbear forçado* consiste no corte da barba, ou depilação de outras partes do corpo, sendo que o relatório admite que esta técnica poderá violar os direitos religiosos de um detido, ao abrigo da Convenção de Genebra, podendo constituir um ultraje à dignidade humana, sendo visto como desumano ou degradante (p. 40).

Ressalva-se que o relatório, por diversas vezes, elenca as questões legais associadas às práticas dos métodos assinalados, nomeadamente fazendo menção às limitações impostas pelas Convenções de Genebra e de Haia e outros quadros normativos associados aos Direitos Fundamentais e do Homem. No entanto, e de modo algo controverso, o Report RL32567

assume que algumas pessoas argumentam que as técnicas descritas equivalem a atos de tortura, contra argumentando que os funcionários do Pentágono haviam declarado que tais métodos poderiam ser aplicados dentro da estrutura da Convenção de Genebra, desde que as necessidades físicas básicas do detido fossem atendidas (p. 32). Constata-se aqui uma exploração metodológica das forças armadas norte-americanas e, por inerência, do próprio poder executivo, do vazio legal proporcionado pela Convenção de Genebra, com quase setenta anos de existência, fazendo a sua interpretação altamente extensiva.

3.3.3. CENTRAL INTELLIGENCE AGENCY(CIA)

Relativamente aos métodos HUMINT aplicados pela agência norte-americana de maior renome, especialmente no que diz respeito ao desenvolvimento das suas ações encobertas e clandestinas, diversas fontes se apresentaram, sendo algumas cientificamente contestáveis, nomeadamente relatos de alegados ex-operacionais da CIA, em formato de monografias romanceadas. Tem-se consciência que tais relatos íntimos poderão ilustrar algumas das práticas reais em uso na CIA, no entanto, tais não foram considerados.

No que diz respeito às práticas de interrogatório da CIA, em cenário de contraterrorismo, o documento “*Guidelines on Medical and Psychological Support to Detainee*” (Central Intelligence Agency, 2003)⁵⁹ elenca-as, sendo perceptível que são, de alguma forma, similares às relatadas anteriormente, em prática pelas forças militares, no contexto de produção de inteligência tática. São estas o *barbear do detido, retiradas das roupas, colocação de fralda (até 72 horas), colocação de um capuz, isolamento, ruído/música elevada, temperatura desconfortável, restrição de dieta* (com redução calórica, suficiente para a manutenção da saúde), *algemagens em posição de desconforto, privação do sono (até 72 horas), imobilização da cabeça, estaladas faciais ou abdominais, detenção em caixas confinadas ou simulações de afogamento (waterboarding)*. Como é constatável, também estes poderão ser interpretados como atos de tortura, censurados pela comunidade internacional (Central Intelligence Agency, 2003, pp. 8-9).

O documento refere que estas práticas deverão ser aplicadas a terroristas capturados e

⁵⁹ Salienta-se que o documento analisado é disponibilizado abertamente pelo arquivo eletrónico pela própria agência.

entregues à CIA para interrogatório, procurando maximizar o seu sentimento de vulnerabilidade e desamparo, reduzindo ou eliminando a sua vontade de resistir aos esforços de obtenção de inteligência, por parte dos interrogadores. O documento reitera, no entanto, que este conjunto de técnicas deverá ser especificamente aprovado pelo Diretor (depreende-se Diretor da CIA) de forma casuística (Central Intelligence Agency, 2003, p. 8). Sob forma alguma, deverão estas técnicas incidir na integridade física do detido, mas sim na psicológica, dando o documento o exemplo das estaladas, que deverão promover somente o choque, a surpresa e/ou a humilhação, e não a lesão física⁶⁰ (Central Intelligence Agency, 2003, p. 10).

Na vertente da penetração HUMINT, sem recurso ao interrogatório de suspeito detidos, nomeadamente através da ação encoberta, Johnson (2010, pp. 312-313) descreve o ciclo de aquisição de informações pela via HUMINT da CIA, de uma forma genérica, sendo, no entanto, aplicável no contraterrorismo. Esclarece que o primeiro objetivo da ação é a identificação das pessoas que possam ter bons acessos às informações/segregados do governo/organização em foco, compreendendo se essas mesmas pessoas poderão ser vulneráveis ao recrutamento. Seguidamente, se confirmadas essas duas características, o próximo passo será a conquista da empatia da fonte, ganhando a sua confiança com um “ouvido compreensivo”. Este processo poderá demorar meses, ou mesmo anos, consoante a permeabilidade do potencial recrutado, podendo, inclusivamente, exigir a coordenação de dois ou mais *case officers* (operacionais HUMINT) em sucessão, convertendo uma potencial fonte numa fonte ativa.⁶¹

No curso da ação de penetração, pela via do recrutamento, se o *case officer* considerar que a ação poderá ser arriscada, no que ao grau de sucesso de recrutamento previsível diz respeito (condicionada pela eventual vulnerabilidade da cobertura do *case officer*), poderá ser usado um intermediário local, confiável por ambas as partes, também designado de *cut-out*. Sendo uma ação arriscada, também em matéria de segurança para ambas as partes, o recrutamento é usualmente recusado pelo alvo, sendo-o por vezes de uma forma pública, podendo, em último

⁶⁰ Aqui, contrariamente ao manual FM 2-22.3– Human Intelligence Collector Operations (2006), abordado anteriormente, a CIA legitima a exploração psicológica do interrogado. O manual militar não admite essa possibilidade.

⁶¹ O autor, na temática da recolha de informações estratégicas dá um exemplo aplicado pela CIA, em contexto genérico. Este esclarece que se eventualmente a empatia surgir e a confiança for mútua, entre o *case officer* e a fonte, é oferecido pelo primeiro um “fundo de investigação” confidencial para preparação de um trabalho de investigação. Se a iniciativa for aceite, então, a porta abre-se para posteriores “fundos de investigação mais avultados” com a contrapartida de uma pesquisa, por parte da fonte, mais sensível. (Johnson L. , 2010, p. 313)

caso, chegar ao meios de comunicação social, comprometendo a cobertura do *case officer* e a credibilidade e reputação da própria CIA. Assim sendo, atendendo à panóplia de vulnerabilidades adjacentes ao recrutamento de fontes, as abordagens aos alvos deverão ser cautelosas, reconhecendo que as fontes são corruptíveis, chegando, de um modo surpreendentemente alto, a converter-se em agentes duplos (Johnson L. , 2010, p. 313).

A CIA, num plano que acaba por extrapolar a ação de produção de inteligência, exerce também missões de natureza análoga à militar (designadas de paramilitares), na vertente “clandestina”⁶². Essas ações, ofensivas e armadas, têm visado influenciar condições políticas, económicas e militares no estrangeiro sem que o papel do governo norte-americano seja aparente ou reconhecido publicamente. A *Special Operations Division* (SAD), criada em 1947, passou a ter maior preponderância nas ações contraterroristas a partir do 11 de setembro (Graça, 2010, p. 248).

3.4. PRÁTICAS BRITÂNICAS

3.4.1. BRITISH ARMY

Um documento parcialmente clarificador do *modus operandi* militar britânico em matéria de produção de inteligência operacional, e, em específico, das práticas de HUMINT, é o *Army Field Manual, Part 3 – Intelligence, Surveillance, Target Acquisition and Reconnaissance*, também abreviado de ISTAR (2002). Foi possível obter este manual através da plataforma *Wikileaks*, sendo que, atendendo à natureza do documento, à forma como se apresenta e à matéria pormenorizada que contém, considera-se um documento fidedigno e efetivamente ilustrativo do conteúdo almejado.

Este manual tem como objetivo, segundo o mesmo, uniformizar procedimentos no campo da aquisição, processamento e disseminação de informações e inteligência atempadas, precisas e relevantes, apoiando estas o planeamento, a conduta de operações, a localização e integração de efeitos, permitindo aos comandantes (militares) o alcance dos objetivos em todo o espectro

⁶² Vista como instrumento de ação encoberta por Shulsky & Schmitt (2002, p. 89). Uma vez mais assinala-se dicotomia conceptual constatada em diferentes autores.

de conflitos⁶³ (p. 7). O ISTAR não se foca exclusivamente no contraterrorismo, mas, atendendo ao empenhamento do exército britânico ser, em grande medida, destinado à ação internacional concertada contra a ameaça terrorista, a partir de 2001, fora do espaço territorial britânico, é este, essencialmente, um manual aplicável ao contraterrorismo.⁶⁴

O ISTAR esclarece que a utilização da HUMINT, nas ações militares britânicas, tem uma aplicabilidade e utilidade condicionada ao tipo de operação em curso, sendo, quando utilizada, uma forma complementar de pesquisa de informações às outras disciplinas. Assume a particular utilidade da HUMINT nas ações de suporte à segurança dos ativos militares e nas ações de contrainteligência (p. 83). Em termos procedimentais, o ISTAR, no que à HUMINT diz respeito, segrega-a em duas tipologias de atividades: as *operações com fontes humanas* e as *operações de apoio às primeiras* (p. 83).

Quanto às *operações com fontes humanas*, o ISTAR caracteriza-as como aquelas que envolvem contacto interpessoal estruturado entre o operacional de HUMINT (devidamente formado) e um indivíduo com acesso a informações com potencial interesse em matéria de inteligência. Estas operações revestem um grau elevado de complexidade, podendo a sua sensibilidade inerente resultar numa necessária atuação encoberta. O manual fragmenta as operações com fontes humanas em cinco subtipos: as de *atividade direta convencional*, as de *ligação*, as de *debriefing*, as de *gestão de fontes* e as de *interrogatório* (p. 83).

A *atividade direta convencional* (que não se poderá designar de operação, propriamente dita) é desenvolvida por elementos militares regulares, não especialistas, onde as informações recolhidas são um produto das suas incumbências quotidianas. Será exemplo desta uma conversa inopinada com a população local, aquando de um patrulhamento numa manobra militar terrestre. As operações de *ligação* consistem no contacto (não encoberto) de operacionais HUMINT, ou de oficiais de inteligência, com membros das organizações aliadas. Serão exemplo destas organizações as polícias, os serviços de inteligência ou outras agências oficiais locais. As operações de *debriefing* dizem respeito às inquirições formais e

⁶³ O ISTAR, com aplicabilidade no exército do RU, será essencialmente utilizado pelo *Intelligence Corps* desse ramo militar, sendo este o serviço responsável pela pesquisa de informações e análise de inteligência (British Army, 2020).

⁶⁴ Segundo o *website* do exército britânico, o Afeganistão (sob coordenação da OTAN) e o continente africano são atuais espaços de intervenção militar britânica, sendo aí o enfoque direcionado para a ameaça terrorista (não exclusivamente, no caso africano) (British Army, 2020).

detalhadas de cidadãos locais selecionados, mediante o consentimento destes, que previsivelmente providenciarão informações de relevo. O ISTAR indica como exemplos os refugiados de uma zona de conflito, membros de uma ONG ou desertores de organizações hostis (pp. 83-84).

As operações de *gestão de fontes*, são caracterizadas como gestão de pessoas que tenham acesso, ou potencialmente poderão tê-lo, a informações significativas (com valor de inteligência), onde os riscos envolvidos são elevados, requerendo este tipo de operações o emprego de operacionais de HUMINT especializados e de técnicas específicas⁶⁵. Dada a sensibilidade deste tipo de operações, o ISTAR salienta que as mesmas requerem autorização ministerial *à priori*, em sujeição escrupulosa ao quadro legal britânico (p. 85). As ações de *interrogatório*, não encobertas, são descritas como questionamento sistemático e formal de indivíduos detidos, num ambiente cuidadosamente controlado. São utilizadas, essencialmente, em prisioneiros de guerra ou membros detidos de organizações hostis às forças britânicas, como serão exemplo disso membros de organizações terroristas. O manual afirma que este tipo de ações deverá ser aplicado por elementos treinados, com capacidade de relevo no âmbito dos conhecimentos linguísticos (p. 84).

Relativamente ao segundo tipo de operações, as *de apoio às anteriores*, o ISTAR segrega-as em dois tipos: as de *reconhecimento de inteligência militar* e as de *vigilância passiva encoberta*. As de *reconhecimento de inteligência militar* são aquelas onde especialistas de HUMINT, fora da área geográfica de intervenção militar (nas imediações), procuram detetar elementos informativos específicos, usualmente de natureza sensível e que possam requerer confirmação ou pesquisa aprofundada posterior. Poderão ser vistos como varrimentos exploratórios. Quanto às operações de *vigilância passiva encoberta*, o manual descreve-as como as de observação sistemática e encoberta, de uma pessoa, sítio ou objeto, a partir de um ponto de vigilância estático ou móvel (através de viaturas ou de forma apeada). Estas, sempre na perspetiva de apoio às operações de inteligência com fontes, acima descritas, poderão prolongar-se por lapsos temporais extensos, visando detetar ou identificar eventos ou determinar padrões comportamentais (p. 84).

⁶⁵ O manual não especifica se a gestão de fontes é desenvolvida de forma encoberta ou não. Contrariamente ao manual militar norte-americano, analisado anteriormente, o FM 2-22.3– *Human Intelligence Collector Operations* (2006), o ISTAR não pormenoriza o procedimento de gestão de fontes humanas.

O manual ISTAR, por fim, acaba também por avaliar as vantagens e desvantagens na aplicação de atividades HUMINT. Atribui como vantagem o facto de as informações estarem mais rapidamente disponíveis, em comparação com as outras disciplinas de pesquisa. Permite ainda, que os requisitos de inteligência possam ser trabalhados em profundidade pelos operacionais de HUMINT (podendo fazer perguntas complementares por iniciativa própria). Possibilita, também, o facto de as operações de HUMINT serem menos dispendiosas, em comparação com outras disciplinas de pesquisa mais tecnológicas. No espectro das desvantagens, esclarece que as operações de HUMINT são tanto mais limitadas quanto maior for a perigosidade do cenário. No âmbito da comunicação entre o operacional e a fonte, os requisitos linguísticos são imprevisíveis, pelo facto de por vezes existir uma elevada imprevisibilidade associada à HUMINT (no que diz respeito ao grau de desenvolvimento da relação entre a fonte o operacional) (pp. 84-85).

3.4.2. SECURITY SERVICE (MI5)

O MI5, enquanto serviço de produção de inteligência de segurança, tem como primordial enfoque o contraterrorismo, em muito definido pelos atentados sofridos pelo RU, de inspiração *jihadista*, nas últimas duas décadas, assumindo o “serviço” esta tipologia de terrorismo como uma ameaça a longo prazo e não como uma vaga passageira (Andrew, 2010, p. 828) ⁶⁶. Não exclui também aqueles de índole separatista, como os perpetuados pelo IRA. Dedicar-se cumulativamente à contra-espionagem, contra-proliferação de armas de destruição em massa e a cibersegurança (MI5, Counter-terrorism, 2020).

Em matéria de pesquisa de informações, o MI5, surpreendentemente, e contrariamente a outros serviços congéneres, opta por uma abordagem de transparência, no que aos seus métodos diz respeito, plasmando-os no seu *website*⁶⁷. Indica que as principais técnicas para a recolha de informações (não pormenorizando o processo posterior de produção de inteligência) são a *utilização de fontes HUMINT*, a *vigilância direccionada*, a *interceção de*

⁶⁶ Andrew (2010, p. 827) ilustra o relevo dado ao terrorismo por parte do MI5, a partir do 11 de Setembro de 2001, quando afirma que até a essa data o RU tinha identificados 250 indivíduos com ligações ao terrorismo internacional (essencialmente de matriz islâmica), sendo que, em 2007, já eram 2000 os indivíduos conotados, estando, inclusivamente, 30 focos de ação terrorista sob investigação. Acrescenta ainda que em 2009, 200 eram as investigações em curso (associadas ao terrorismo de matriz islâmica), onde 15% dessas estavam classificadas de nível de ameaça elevado (2010, p. 833).

⁶⁷ Existindo a plena consciência que o elenco é exposto de modo generalista, não dando azo à compreensão de especificidades operacionais.

comunicações, análise de metadados, a recolha de dados pessoais em massa, a vigilância intrusiva e a interferência de comunicações (MI5, 2020).

Este serviço de inteligência esclarece que a pesquisa de informações com recurso as *fontes HUMINT* são os agentes (apelidados de *agents*⁶⁸), geridos durante longos períodos por *agents handlers* (oficiais de inteligência), que fornecem informações secretas sobre um alvo de uma determinada organização, considerando-os o MI5 uma das mais importantes formas de pesquisa de informações. Define a *vigilância direcionada* como aquela onde os alvos pesquisados são perseguidos e observados, analisando os seus movimentos, conversações ou outras atividades. Caracteriza a *interceção de comunicações*, como o próprio conceito indica, como a monitorização de emails, de mensagens ou de chamadas de voz provenientes de telefones ou telemóveis. Descreve a *análise dos metadados* como a recolha em massa de informações sobre a realização das próprias comunicações, nomeadamente como, onde e quando foram realizadas, sendo estes dados provenientes das operadoras telefónicas (MI5, 2020).

Por sua vez, aclara que a *recolha de dados pessoais em massa* é realizada através de bases de dados detentoras de uma grande quantidade de informações, sobre pessoas que possam, de alguma forma, estar correlacionadas com matérias em interesse do “serviço”. Clarifica que *vigilância intrusiva* dever-se-á entender como a colocação de dispositivos tecnológicos em espaços ocupados ou utilizados pelo alvo, como a sua residência ou carro, capazes de recolher elementos fotográficos, videográficos, sonoros, geográficos ou outros. Conclui, explicando que a *interferência de comunicações*, também designada de exploração de redes informáticas, é o acesso encoberto a computadores, ou outros dispositivos detentores de elementos informativos, com o propósito de obter informações sobre as comunicações efetuadas, ou outras armazenadas nesses suportes (MI5, 2020). Nos métodos listados, denota-se a

⁶⁸ Relativamente a esta designação, no contexto britânico, “agente” é a pessoa recrutada pelo oficial de inteligência, não se podendo afirmar que são funcionários dos serviços de inteligência. O mesmo acontece na restante Europa, onde o “agente” é sempre aquele que é externo e fornece informações ao oficial de informações. É o exemplo da Rússia, que define “agente” como o indivíduo que conscientemente, sistematicamente e clandestinamente realiza tarefas de inteligência em cooperação secreta com um representante de um oficial de inteligência ou um representante de uma organização (às vezes lendária), em que o oficial de inteligência ou o agente desempenham uma parte secreta (Mitrokhin, 2002, p. 3). Já nos EUA existe uma dualidade semântica quanto ao termo “agente”. A maioria das fontes (algumas de organismos oficiais) sugerem que o “agente” é aquele que é funcionário do serviço de inteligência, como é exemplo o *Intelligence Branch* do FBI (Federal Bureau Investigation, 2020), apesar da CIA, assim como outros organismos, já reservarem o termo “agente” para as fontes recrutadas, designando os seus funcionários como *officers*.

preponderância do homem na recolha de informações, sendo a HUMINT, aparentemente, a valência preferencial do MI5.

O MI5 pormenoriza as formas de pesquisa de informações, sem deixar, no entanto, de realçar que estão legalmente previstas pelo *Security Service Act* de 1989⁶⁹, o *Intelligence Services Act* de 1994⁷⁰, o *Regulation of Investigatory Powers Acts* de 2000⁷¹ e os códigos práticos impostos legalmente⁷². Salienta, também, o escrutínio do *Interception Communications Comissioner*⁷³, em matéria de interceção de dados comunicacionais, designadamente da utilização de escutas e análise de metadados. O MI5, sobre os métodos de pesquisa mais intrusivos, afirma que são usados com moderação, somente em casos de maior complexidade, onde outros meios menos devassadores não sejam suficientes, dando o exemplo da aplicação das escutas (MI5, 2020).

O MI5, contrariamente aos restantes serviços de inteligência/forças militares abordadas, aplica uma abordagem inovadora e complementar, no que diz respeito ao recrutamento de fontes. Para além do tradicional, e já descrito anteriormente, processo de recrutamento de fontes humanas, o MI5, no seu próprio *website*, desenvolve uma ação de recrutamento massiva, dirigida a qualquer pessoa que consulta o mesmo, especialmente no que diz respeito à ameaça contraterrorista. Este serviço de inteligência assinala que qualquer membro do público poderá ajudar a prevenir atos terroristas, estando alerta para potenciais atividades

⁶⁹ Lei estatutária do MI5 (Legislation.gov.uk, Security Service Act 1989, 2020).

⁷⁰ Lei estatutária do SIS e GCHQ (Legislation.gov.uk, 2020).

⁷¹ O *Regulation of Investigatory Powers Act 2000*, na sua segunda parte, regulamenta o uso da vigilância encoberta por órgãos públicos, incluído a utilização de *bugs*, vigilância por vídeo, interceção de comunicações (telefónicas ou eletrónicas) e a utilização de agentes encobertos (fontes humanas recrutadas) (Justice, 2020).

⁷² Salienta-se que o RU detém dois manuais práticos no âmbito das atividades de inteligência encoberta: o *Covert Human Intelligence Sources - Revised Code of Practice* (Home Office, 2018) e o *Covert Surveillance and Property Interference - Revised Code of Practice* (Home Office, 2018). O primeiro, segundo o próprio, providencia orientação no processo de autorização para a utilização ou condução de fontes humanas encobertas por autoridades públicas, ao abrigo da *Part II* do *Regulation of Investigatory Powers Act 2000* (Home Office, 2018, p. 7). O segundo, também consoante o manual em si, providencia orientação no processo de autorização de vigilâncias encobertas, ao abrigo da *Part II* do *Regulation of Investigatory Powers Act 2000*, que potencialmente possam resultar na obtenção de informações subjacentes ao foro privado de uma pessoa (Home Office, 2018, p. 8).

⁷³ O *Interceptions Communications Comissioner*, substituído pelo atual *Investigatory Powers Comissioner's Office* é o organismo independente que supervisiona os poderes de investigação das agências de inteligência, forças policiais e outras autoridades públicas (Investigatory Powers Comissioner's Office, 2020).

suspeitas, através de um discurso informal, direto e de alguma forma emotivo, envolvendo assim a comunidade britânica⁷⁴ (MI5, 2020).

Este serviço vai ainda mais longe quando no recrutamento de agentes através do seu *website*, cria uma página dedicada somente às questões que os agentes regularmente têm ou que possam vir a ter, aquando do processo de recrutamento ou de colaboração espontânea com aquele serviço de inteligência. Começa por clarificar que qualquer pedido que o serviço faça ao agente será cuidadosamente planeado para minimizar os potenciais riscos, sendo que nunca nenhum agente será compelido a fazer coisas que não queira. Esclarece que o mais importante será a relação de confiança e honestidade entre ambos (o agente e o *case officer*), sendo que será discutida a melhor forma para atingir o objetivo do serviço e, por inerência, do RU. Salienta que os gestores de fontes detêm um grau elevado de formação, em especial no que à deteção de riscos diz respeito (MI5, 2020).

Posteriormente, de uma forma novamente emotiva, apelando ao patriotismo, assinala que o serviço não conseguirá manter o RU seguro sem a colaboração dos cidadãos que possam providenciar informações vitais que sejam capazes de anular uma ação terrorista. Em seguida, não deixando esta questão para o fim, dando-lhe relevância, e conseqüentemente não perdendo potenciais fontes a meio da leitura da página do *website*, o MI5 informa que existem muitas formas de reconhecimento da importância do papel destes agentes, nomeadamente através da compensação pecuniária.⁷⁵ Salienta, no entanto, que outras formas de compensação poderão existir. Relativamente à privacidade do contacto, o serviço esclarece que essa será garantida e que a relação entre o gestor de fontes e o agente será limitada e que nunca será confirmada publicamente, pedindo também para que essa confidencialidade se aplique em sentido contrário, que o agente limite a difusão daquilo que foi transmitido ao gestor de fontes (MI5, 2020).

⁷⁴ “*Terrorists have to live somewhere, and they need to plan and prepare for attacks. They buy and store materials, fund their activities, move around, prepare equipment and weapons and possibly undergo training. They may have people helping them - and these people might come and go at strange times of the day and night. They may make unusual financial transactions or use false documents to hide their real identities. They may be behaving differently from how you've known them to behave in the past. Members of the public may spot such activities, and if reported in time, a planned terrorist attack may be stopped before it happens(...)*If you are aware of something suspicious, trust your instincts and report it to the police. What might seem insignificant on its own could actually provide a vital link in a wider investigation” (MI5, 2020).

⁷⁵ “...we would certainly not expect someone to be out of pocket for agreeing to help” (MI5, 2020).

O MI5 reitera que o agente só falará e fará aquilo que quer, sendo que ninguém o irá forçar a colaborar, em determinado momento. Uma vez mais, recorrendo à emoção, e apesar da ação do agente ser voluntária, apela ao humanismo da potencial fonte, dizendo que esta poderá estar numa posição única para fornecer informações relevantes que manterão o RU seguro e que aquilo que eventualmente será pedido poderá ser crucial para a preservação de vidas humanas. Relativamente ao eventual passado criminal do agente ou afinidades extremistas do mesmo, o MI5 indica que não existirá qualquer obstáculo nesse aspeto, sendo que, acima de tudo, necessitam de falar com pessoas que compreendam a realidade subjacente à ameaça pesquisada pelo serviço. De um forma conclusiva, e dirigindo-se para a comunidade em geral, o MI5 clarifica que não investiga toda a comunidade do RU, mas sim aqueles indivíduos que possam potencialmente estar a planear atos que possam lesar a sociedade em geral, como os de natureza terrorista, ou outros indivíduos, que, não estando a planear atos de natureza terrorista, os possam financiar ou apoiar materialmente (MI5, 2020).

Poder-se-á concluir que esta inovadora forma de recrutamento de fontes poderá trazer inúmeras vantagens a um serviço de inteligência, nomeadamente no que diz respeito ao incremento exponencial das informações recolhidas. O esclarecimento providenciado pelo próprio serviço, do modo como as fontes são geridas, também desmistificará alguns preconceitos que possam existir, motivando potenciais fontes que até aqui poderiam, de alguma forma, estar receosas ou condicionadas a facultar informações (pela perspetiva de insegurança, desconfiança nos próprios serviços ou preconceção que daquela colaboração não adviria compensação monetária alguma).

No entanto, considera-se que a vulnerabilidade deste método passará pela dificuldade na filtragem das informações extraídas pela via HUMINT, já que o número de agentes poderá incrementar significativamente, conduzindo, inevitavelmente, a um exponencial da desinformação. Outra vulnerabilidade será o eventual malefício que poderá existir aquando da exposição do *modus operandi* do MI5, em matéria de recrutamento de fontes, perdendo-se a vantagem estratégica, subjacente ao secretismo, e inerente desconhecimento do adversário. Considera-se que, apesar destas vulnerabilidades, esta prática de transparência e clarificação metodológica, conduzirá a uma maior aceitação dos cidadãos britânicos do trabalho desenvolvido por este serviço de inteligência (onde naturalmente a desconfiança está presente) e conseqüente incremento da participação ativa nas tarefas de pesquisa do serviço,

sendo maior o benefício do que o prejuízo. Denota-se, aqui, um desvanecer gradual do secretismo subjacente ao *core business* dos serviços de inteligência.

CONCLUSÕES

Esta investigação permitiu compreender que a pesquisa HUMINT contemporânea é essencialmente posta em prática pela via da penetração (ou recrutamento). De todos os elementos primários que foi possível analisar, nenhum deles pormenoriza metodologias de infiltração em organizações terroristas, ou em meios sociais onde poderão estar indivíduos terroristas inseridos. A conclusão que se poderá extrair desta ausência de elementos caracterizadores das práticas de infiltração é que, dada a natureza cultural altamente díspar das organizações terroristas de matriz islâmica (tipologia de maior ênfase no mundo ocidental, hodiernamente), em matéria de fisionomia, linguagem, comportamentos ou hábitos, dificulta a infiltração de elementos das FSSD. A penetração, através do recrutamento de fontes inseridas na organização ou com contacto privilegiado com elementos da organização será mais viável, menos arriscado e com um potencial de sucesso superior.

Como afirma Wagner (2011, p. 54), a maioria das células terroristas são, hoje em dia, altamente compartimentadas, normalmente compostas por amigos e familiares chegados, inviabilizando a infiltração. A forma mais produtiva será o recrutamento de fontes pertencentes ou próximas à célula terrorista através do suborno, correndo, mesmo assim, o risco de os elementos informativos cedidos serem falsos ou desorientadores. Também Carrol (2002, p. 2) defende que, dada a compartimentação anteriormente elencada e a natureza violenta dos grupos terroristas mais preponderantes, atualmente, como o ISIL ou a *Al Qaida*, mesmo a penetração provavelmente revestirá um insucesso. O autor contrapõe, no entanto, que esta é a melhor forma de alcançar a precisão das informações recolhidas, desde que o contacto entre um operacional de pesquisa e uma fonte recrutada ocorra de forma encoberta. Ou seja, se por um lado o sucesso das ações de HUMINT, seja pela via da infiltração, seja pela via da penetração, é significativamente limitado, por outro, a segunda forma será a melhor forma (ou “menos má”) de obter conteúdos precisos, conduzindo à produção de inteligência com valor acrescentado. A pesquisa HUMINT reveste um risco elevado, mas a recompensa, também ela, é elevada.

Atendendo ao afunilamento das práticas de HUMINT analisadas para a vertente da penetração (recrutamento), escrutinou-se, no espectro norte-americano, um manual de procedimentos HUMINT do exército, debruçado no processo de pesquisa HUMINT em geral, um relatório

sobre práticas HUMINT do Departamento de Defesa, recaindo sobre a vertente de interrogatório a detidos, e um manual de intervenção com detidos da CIA, também no campo do interrogatório. No plano do RU, examinou-se um manual de procedimentos HUMINT do exército, focado nas atividades com fontes humanas em geral, e analisou-se o website da MI5, com a sua *sui generis* ação de recrutamento em meio aberto. Salienta-se que, apesar de qualquer uma destas fontes não se versar de modo exclusivo no combate ao terrorismo, é notório que o principal enfoque recai nesta temática, dadas as alusões permanentes ao fenómeno em si.

Com o manual de HUMINT do exército norte americano, FM 2-22.3– Human Intelligence Collector Operations (2006), foi possível compreender as metodologias utilizadas por aquela força militar no plano de recrutamento de fontes, desde as fases mais primárias de seleção dos alvos até à extração dos elementos informacionais almejados. Com o relatório de práticas HUMINT do Departamento de Defesa do EUA, Report RL32567 (2004), escrutinador das práticas controversas de interrogatório de Abu Graib e com o manual de intervenção da CIA, *Guidelines on Medical and Psychological Support to Detainee Interrogation* (Central Intelligence Agency, 2003), conheceu-se os distintos métodos de interrogatório a detidos e as circunstâncias de aplicação de cada um deles. Foi possível, por um lado, perceber as vantagens e desvantagens de cada um dos métodos, atendendo às suas especificidades e eficiência com as fontes, e, por outro, detetar a existência de práticas controversas e alegadamente violadoras do Direito Internacional Público, nomeadamente o que diz respeito aos Direitos Fundamentais do Homem. No entanto, nunca foi intenção desta investigação debruçar-se sobre aspetos legais ou éticos, mas sim nos procedimentais.

Por sua vez, a análise do manual de HUMINT do exército britânico permitiu compreender as modalidades daquela força militar no plano da pesquisa de informações pela via humana, desde as operações convencionais de pesquisa, às de gestão de fontes, passando pelas de ligação ou de interrogatório. Foi possível compreender as vantagens e desvantagens de cada modalidade, apreciadas pelo próprio manual. Quanto à análise do *website* do MI5, esta relevou-se de elevado interesse, tendo em conta o facto daquele serviço de inteligência desenvolver uma ação de recrutamento de fontes, essencialmente no plano do contraterrorismo, de forma aberta e transparente. Foi possível compreender como o MI5, de

forma apelativa, patriótica e quase emotiva, dirige uma ação massiva de recrutamento a todos os cidadãos detentores de potenciais informações de relevo.

Este trabalho promoveu uma caracterização sistemática das práticas de HUMINT em contexto de contraterrorismo, contribuindo para o conhecimento ainda limitado e muitas vezes especulativo nesta temática, congregando elementos primários e secundários distintos, promovendo um quadro, naturalmente incompleto, de práticas diversificadas das FSSD anglo-americanas. Permitiu a compreensão dos métodos e da sua eficácia, perante os alvos assinalados, descortinando um pouco mais daquilo que continua a ser matéria classificada das organizações produtoras de inteligência contraterrorista. No entanto, muito mais haverá a descortinar e a compreender, sendo que, no futuro, esta deverá ser uma temática a aprofundar, permitindo, por um lado, esclarecer a comunidade científica, em específico, e a sociedade, em geral.

Não nos poderemos, no entanto, dissociar do duplo efeito do aprofundamento do conhecimento nesta área. Por um lado, será benéfico conhecer, tornar mais transparente e, acima de tudo, fundamentar o porquê da utilização destas práticas, por vezes interpretadas de forma errónea pelo cidadão alheado dos riscos de segurança proporcionados pelo terrorismo. Por outro, poderá ser prejudicial este conhecimento por parte dos atores subversivos, munindo-os de elementos informativos que poderão ser úteis na sua adaptação de atuação, e, em consequência disso, suprimir a vantagem estratégica das FSSD, altamente dependente da surpresa.

Considera-se que, olhando às duas consequências do aprofundamento científico nesta área, a primeira deverá sobrepor-se à segunda. Apesar de a vantagem estratégica poder sair melindrada, será sempre benéfico saber mais sobre o tema, esclarecendo a sociedade (limitando a especulação) e, no nosso ponto de vista, o aspeto mais importante, alimentar outras FSSD, de distintas partes do globo, de *know-how* técnico, que por outra forma não teriam acesso. Considerando a natural reticência na partilha de inteligência entre FSSD, seja ao nível doméstico, seja no plano internacional, a investigação científica poderá assumir parte desse papel de formação profissional de operacionais nesta área de intervenção contraterrorista, de uma forma não convencional. De modo a salvaguardar ao máximo a vantagem estratégica que as FSSD deverão deter na sua ação de combate ao terrorismo, a

investigação neste campo deverá procurar preservar elementos pormenorizados (caso os conheça) sobre a identidade dos intervenientes, localizações geográficas precisas ou outros pormenores de atuação meramente secundários (mas denunciadores).

Em jeito de conclusão, compete-nos analisar de forma prospetiva a atividade de HUMINT no contraterrorismo. Indubitável será afirmar que a HUMINT sempre teve um papel fundamental no combate ao terrorismo, dadas as informações detalhadas adquiríveis por esta via. A HUMINT tem permitido, e irá continuar a permitir, em primeira mão, estabelecer contactos privilegiados com membros de organizações terroristas ou outras pessoas intermediárias desses membros, promovendo conhecimento com um nível de detalhe não atingível pelas outras disciplinas de pesquisa de informações.

Também se poderá afirmar, em contraposição, que o terrorismo contemporâneo com maior mediatismo, e causador do maior número de fatalidades, o de matriz islâmica, apesar de não ser necessariamente o que ocorre com maior frequência nos espaços geográficos analisados, é mais complexo em termos de infiltração ou penetração, por parte das sociedades ocidentais. Dada as diferenças raciais, étnicas, religiosas e culturais, é dificultada a penetração por FSSD, impossibilitando ainda mais a infiltração. A familiaridade entre os membros destas organizações é relevante, limitando assim a capacidade de extração de informações credíveis, que não se venham a revelar enquanto atos deliberados de desinformação.

No entanto, tendo em conta que a sociedade global atual (onde se incluem as organizações terroristas, ou atores terroristas solitários) tem perfeita consciência da vulnerabilidade subjacente às comunicações telefónicas e eletrónicas, dada a capacidade técnica de interceção por parte das FSSD, ou de vigilância aérea com o recurso a *drones*, ficam assim limitadas as disciplinas de pesquisa SIGINT ou IMINT. As FSSD não poderão assumir que a HUMINT será relegável para um segundo plano, em detrimento das outras disciplinas tecnologicamente evoluídas. À semelhança do “pequeno criminoso de rua”, do traficante de armas ou de droga à escala internacional, as organizações terroristas vão cada vez mais voltar a comunicar entre si por meios ancestrais, descartando os meios de comunicação à distância, passíveis de ser intercetadas as informações transmitidas. A consequência desse regresso ao passado será a conversão da TECHINT num método de pesquisa parcialmente obsoleto. O mesmo ocorrerá

com a OSINT, pois aquilo que é estrategicamente crucial para as organizações terroristas, jamais será divulgado em regime aberto.

A TECHINT e a OSINT não deixarão de ser métodos úteis de pesquisa de informações, sendo que deverão ocorrer em regime de fusão com a HUMINT. Ou seja, a OSINT sinalizará, de um modo prévio, o fenômeno terrorista a conhecer, podendo ser um auxiliar intraprocessual, e a TECHINT instrumentará as ações de recrutamento ou de infiltração, se tal for viável. Na nossa convicção, tendo por base o manancial de elementos congregado na presente dissertação, o futuro da inteligência contraterrorista deverá passar pelo enfoque na HUMINT coadjuvado pelas restantes disciplinas de pesquisa, e não o contrário. A evolução tecnológica e a massiva quantidade de elementos informativos presentes na *internet* serão excelentes instrumentos auxiliares, não devendo ser, por si só, decisivos na fase da análise do ciclo de produção de inteligência.

Concluindo, poderá antecipar-se um cenário relativamente desfavorável ao contraterrorismo eficiente. Por um lado, será cada vez mais necessário o recurso à HUMINT, dada a insuficiência da TECHINT e da OSINT (considerando o regresso à articulação das organizações terroristas por vias mais rudimentares), e, por outro, será cada vez mais difícil a infiltração e recrutamento nas tipologias atuais de organizações terroristas com maior preponderância. Caberá assim, às FSSD, desenvolver estratégias que possam contornar esta limitação operacional, procurando aceder às fontes humanas de informações por vias menos convencionais, como será o exemplo da metodologia aplicada atualmente pelo MI5, descrita anteriormente.

Considera-se que o envolvimento da comunidade na partilha de informações, esclarecendo abertamente todos os pormenores subjacentes à relação que se poderá desenvolver entre as FSSD e o “agente”, beneficiará a produção de inteligência eficiente. Tornando qualquer cidadão um potencial recrutado, garantindo a confidencialidade e, se necessário, a compensação pecuniária respetiva, a ação contraterrorista será potenciada. Consequentemente, e em suma, será exponenciado o número de elementos informativos e também a sua qualidade, prevenindo, assim, mais atos terroristas que vão fragilizando os poderes instituídos e a sociedade em geral.

REFERÊNCIA BIBLIOGRÁFICAS

LIVROS E ARTIGOS

- Aid, M. (2009). All glory is fleeting: SIGINT and the fight against international terrorism. In C. Andrew, R. J. Aldrich, & W. k. Wark, *Secret Intelligence* (pp. 40-77). Abingdon: Routledge.
- Albarello, L., Digneffe, F., Hiernaux, J.-P., Maroy, C., Ruquoy, D., & Saint-Georges, P. d. (1995). *Práticas e Métodos de Investigação em Ciências Sociais*. Lisboa: Grávida.
- Almeida, J. F., & Pinto, J. M. (1990). *A Investigação nas Ciências Sociais*. Lisboa: Editorial Presença.
- Alves, A. C. (2010). *Introdução à Segurança*. Lisboa: Revista da Guarda Nacional Republicana.
- Andrew, C. (2010). *The Defense of the Realm. The Authorized History of MI5*. Londres: Penguin Books.
- Assembleia Constituinte. (1976). Constituição da República Portuguesa. Lisboa, Lisboa, Portugal: Diário da República Eletrónico.
- Assembleia da República. (2008). Lei n.º 53/2008, de 29 de agosto de 2008. *Lei de Segurança Interna*: Diário da República Eletrónico.
- Baylis, J., Wirtz, J., & Gray, C. (2002). *Strategy in the Contemporary World: An Introduction to Strategic Studies*. Nova Iorque: Oxford University Press.
- Beaufre, A. (2004). *Introdução à Estratégia*. Lisboa: Edições Sílabo.
- Bellaby, R. (2017). The Ethics of Intelligence. *The Palgrave Handbook of Security, Risk and Intelligence*, pp. 395-409.
- Berkowitz, B., & Goodman, A. (1989). *Strategic Intelligence for American National Security*. Nova Jersey: Princeton University Press.

- Best Jr., R. A. (2010). Intelligence Issues for Congress. In P. R. Haas, *Intelligence Oversight and Disclosure Issues* (pp. 29-52). Nova Science Publishers: New York.
- Bispo, A. d. (2004). A Função de Informar. In A. Moreira, *Informações e Segurança* (pp. 77-104). Lisboa: Prefácio.
- Byman, D. (2013). The Intelligence War on Terrorism. *Intelligence and National Security*, 1-27.
- Cardoso, P. (2004). *As Informações em Portugal*. Lisboa: Grávida.
- Clausewitz, C. v. (1997). *Da Guerra*. Mem Martins: Publicações Europa-América.
- Correia, J. A. (2015). *Conceito Estratégico Nacional. Subsídios para a sua aplicação em Portugal*. Lisboa: Instituto Superior de Ciências Sociais e Políticas.
- Couto, A. C. (1988). *Elementos de Estratégia: Apontamentos para um Curso - Volume II*. Lisboa: Instituto de Altos Estudos Militares.
- Dougherty, J. E., & Pflatzgraff, Jr., R. L. (2003). *Relações Internacionais. As Teorias em Confronto*. Lisboa: Grávida.
- Duarte, A. P. (2013). Estratégia: Origem e Fundamento. *Nação e Defesa, nº136. Estratégia*, pp. 34-65.
- Duque, R. (2016). Terrorismo: um olhar sobre a evolução e as particularidades desta forma de violência política. In R. Duarte, D. Noivo, & T. d. Silva, *Segurança Contemporânea* (pp. 131-150). Lisboa: Pactor.
- Evans, G. (2006). Responding to Terrorism: A Global Stocktake. Em D. S. Hamilton, *Terrorism and International Relations* (pp. 147-158). Lisboa: Fundação Calouste Gulbenkian.
- Fernandes, L. F. (2004). As sociedades contemporâneas e a ameaça terrorista. Em A. Moreira, *Terrorismo* (pp. 461-481). Coimbra: Almedina.
- Fernandes, L. F. (2014). *Intelligence e Segurança Interna*. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna.
- Ganor, B. (2002). Defining Terrorism: Is one man's terrorist another man's freedom fighter? *Police Practice and Research, Vol. 3, Nº 4*, pp. 287-304.

- Godoy, A. S. (1995, 05). Introdução à Pesquisa Qualitativa e as suas Possibilidades. *Revista de Administração de Empresas*, pp. 57-63.
- Goldman, J. (2006). *Words of Intelligence: A Dictionary*. Toronto: The Scarecrow Press, Inc.
- Gómez, A. M. (2007). Doctrina de infiltración para Inteligencia Contraterrorista. *Athena Paper, Vol. 2, No 3 Artículo 1/4*, 1-23.
- Graça, P. B. (2004). Metodologia da Análise nas Informações Estratégicas. Em A. Moreira, *Informações e Segurança. Estudos em Honra do General Pedro Cardoso* (pp. 429-438). Lisboa: Prefácio.
- Graça, P. B. (2010). *Mundo Secreto. História do Presente e Intelligence nas Relações Internacionais*. Instituto de Informações e Segurança de Angola.
- Graça, P. B. (2014). A Área dos Estudos Estratégicos. *Lusiada. Política Internacional e Segurança. Nº 10*, pp. 65-81.
- Green, S. N., & Proctor, K. (2016). *Turning Point. A New Comprehensive Strategy for Counter Violent Extremism*. Washington D.C.: Center for Strategic & International Studies .
- Hoffman, B. (2006). *Inside Terrorism*. Nova Iorque: Columbia University Press.
- ITTACG. (2009). *ITAGG. Intelligence Guide for First Responders*. National Counterterrorism Center.
- Jesus, J. M. (2015). *Espionagem e Contraespionagem em Portugal. Vicissitudes e Mistérios*. Lisboa: Edições 70.
- Johnson, L. (2010). Evaluating “Humint”: The Role of Foreign Agents in U.S. Security. *Comparative Strategy*, pp. 308-332.
- Johnson, L. K. (2007). The meanings of intelligence. In L. K. Johnson, *Handbook of Intelligence Studies* (pp. 1-14). Abingdon: Routledge.
- Johnston, J. M., & Johnston, R. (2005). Testing the Intelligence Cycle Through Systems Modeling and Simulation. In R. Johnston, *Analytic Culture in the US Intelligence Community. An Ethnographic Study* (pp. 45-57). Washington D.C.: Center for the Study of Intelligence.

- Jonhson, L. K. (2009). Sketches for a theory of strategic intelligence. In P. Gill, S. Marrin, & M. Phythian, *Intelligence Theory. Key questions and debates* (pp. 33-53). Abindgon: Routledge.
- Kaplan, R. S., & Norton, D. P. (2008). *The Execution Premium. Linking Strategy to Operations for Competitive Advantage*. Boston: Harvard Business Press.
- Kent, S. (1967). *Informações Estratégicas*. Rio de Janeiro: Biblioteca do Exército - Editora.
- Kerlinger, F. (1979). *Metodologia da Pesquisa em Ciências Sociais*. São Paulo: Editora Pedagógica e Universitária Ltda.
- Krizan, L. (1999). *Intelligence Essentials for Everyone*. Washington: Joint Military Intelligence College.
- Laqueur, W. (1987). *The Age of Terrorism*. Boston: Little, Brown and Company.
- Lara, A. d. (2002). *Imperialismo, Descolonização, Subversão e Dependência*. Lisboa: Instituto Superior de Ciências Sociais e Políticas.
- Lara, A. d. (2007). *O Terrorismo e a Ideologia do Ocidente*. Coimbra: Almedina.
- Lara, A. d. (2011). *Subversão e Guerra Fria*. Lisboa: ISCSP.
- Lara, A. d. (2015). *Ciência Política. Estudo da Ordem e da Subversão*. Lisboa: Instituto Superior de Ciências Sociais e Políticas.
- Larson, E. V., Eaton, D., Nichiporuk, B., & Szayna, T. S. (2008). *Assessing Irregular Warfare. A Framework for Intelligence Analysis*. Santa Mónica: RAND Corporation.
- Loureiro dos Santos. (2001). *Segurança e Defesa na Viragem do Milénio: Reflexões sobre Estratégia II*. Mem Martins: Publicações Europa América.
- Lowenthal, M. M. (2003). *Intelligence: From Secrets to Policy*. Washington: CQ Press.
- Maltez, J. A. (1996). *Princípios de Ciência Política. Introdução à Teoria Política*. Lisboa: Instituto Superior de Ciências Sociais e Políticas.
- Maltez, J. A. (2018). *Manual de Ciência Política. Teoria Geral da República*. Lisboa: Instituto Superior de Ciências Sociais e Políticas.

- Marrin, S. (2007). Adding value to the intelligence product. In L. K. Johnson, *Handbook of Intelligence Studies* (pp. 199-210). Abingdon: Routledge.
- Matos, H. (2012). Contraterrorismo: O Papel da Intelligence na Ação Preventiva e Ofensiva. *VII Congresso Português da Sociologia* (pp. 1-17). Porto: Universidade do Porto - Faculdade de Letras e Faculdade de Psicologia e Ciências da Educação.
- Matos, H. J. (2018). *Terrorismo & Contraterrorismo. Sistemas de Segurança Interna*. Casal de Cambra: Caleidoscópio.
- Mayer, M. A. (2016, 06). Enhanced Human Intelligence Is the Key to Defeating Terrorists. *American Enterprise Institute*, pp. 1-7.
- McDowell, D. (2009). *Strategic Intelligence. A Handbook for Practitioners, Managers and Users*. Toronto: The Scarecrow Press, Inc.
- Mercado, S. (2009). A venerable source in a new era. In C. Andrew, R. J. Aldrich, & W. K. Wark, *Secret Intelligence* (pp. 78-89). Abingdon: Routledge.
- Mitrokhin, V. (2002). *KGB Lexicon: The Soviet Intelligence Officers Handbook*. Londres: Routledge.
- Moore, D. T. (2007). *Critical Thinking and Intelligence Analysis. Occasional Paper Number Fourteen*. Washington D.C.: Center for Strategic Intelligence Research.
- Moreira, A. (2014). *Ciência Política*. Coimbra: Almedina.
- Moreira, C. D. (2007). *Teorias e Práticas de Investigação*. Lisboa: Instituto Superior de Ciências Sociais e Políticas.
- Naghshineh, N. (2008). HUMINT or WEBINT? Concept Study on Possible Routes for Improving Knowledge Discovery Within Organizations. *New Review of Information Networking*, 37-50. Teerão: Routledge.
- Omand, S. D., Barlett, J., & Miller, C. (2012, 09 28). Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security Vol. 27, No 6*, pp. 801-823.
- Pereira, R. (2005). Informações e Investigação Criminal. Em M. G. Valente, *I Colóquio de Segurança Interna* (pp. 25-44). Coimbra: Almedina.

- Phythian, M. (2013). Beyond the Intelligence Cycle. Em M. Phytian, *Understanding the Intelligence Cycle* (pp. 1-6). Abingdon: Routledge.
- Presidência do Conselho de Ministros. (1988, 12 03). Resolução do Conselho de Ministros nº50/88. Diário da República - I Série.
- Quivy, R., & Campenhoudt, L. V. (1992). *Manual de Investigação em Ciências Sociais*. Lisboa: Grávida.
- Ribeiro, A. S. (2010). *Teoria Geral da Estratégia. O Essencial ao Processo Estratégico*. Coimbra: Almedina.
- Ribeiro, A. S. (2016). Os Serviços de Informações no Combate ao Terrorismo Contemporâneo. Ensaio sobre a contenção da ameaça que marca o século XXI. (I. -I. Políticas, Ed.) *Conferências Internacionais sobre Terrorismo Contemporâneo - 2016 - 2017. Uma abordagem ao terrorismo multidisciplinar*, pp. 97-112.
- Ribeiro, A. S. (2017). *O Processo Estratégico na Marinha*. Lisboa: Edições Culturais da Marinha.
- Richard A. Best, J. (2010). Intelligence Issues for Congress. EM P. R. Haas, *Intelligence Oversight and Disclosure Issues* (pp. 29-52). Nova Science Publishers: New York.
- Richelson, J. T. (2007). The Technical Collection of Intelligence. Em L. K. Johnson, *Handbook of Intelligence Studies* (pp. 105-117). Abingdon: Routledge.
- Romana, H. B. (2004). O novo framework do terrorismo internacional de matriz islâmica: desafios ao modelo de análise em informações estratégicas. Em A. Moreira, *Informações e Segurança. Estudos em Honra do General Pedro Cardoso* (pp. 257-270). Lisboa: Perfácio.
- Romana, H. B. (2005). *Terrorismo e "Intelligence": um novo quadro analítico*. Retirado de Janus Anuário: http://www.janusonline.pt/arquivo/2005/2005_4_1_11.html
- Ross, K., & Duchesne, D. (2007). Why feedback is crucial to the intelligence cycle. *Gazette. Vol. 69 n°3*, pp. 32-33.

- Santos, V. M. (2007). *Introdução à Teoria das Relações Internacionais. Referências de Enquadramento Teórico-Analítico*. Lisboa: Instituto Superior de Ciências Sociais e Políticas.
- Schmid, A. P. (2011). The Definition of Terrorism. Em A. P. Schmid, *The Routledge Handbook of Terrorism Research* (pp. 39-98). Abingdon: Routledge.
- Shulsky, A. N., & Schmitt, G. J. (2002). *Silent Warfare. Understanding the World of Intelligence*. Washington, D.C.: Potomac Books, Inc.
- Silva, A. S. (2010). Capacidades e formas de intervenção: a Segurança Interna e Externa; a Cooperação Civil-Militar. Relações entre Segurança e Defesa. *I Congresso Nacional de Segurança e Defesa*. Lisboa: Diário de Bordo.
- Silva, A. S., & Pinto, J. M. (1986). *Metodologia das Ciências Sociais*. Porto: Edições Afrontamento.
- Silva, T. d. (2016). *Islão e Fundamentalismo Islâmico. Das origens ao Século XXI*. Lisboa: Pactor.
- Taylor, S., Bodgan, R., & DeVault, M. (2016). *Introduction to Qualitative Research Methods: A Guidebook and Resource*. New Jersey: John Wiley & Sons Inc.
- Torres, J. E. (2009). *Terrorismo Islâmico: Gestão dos Riscos para a Segurança Nacional*. Lisboa: Universidade Autónoma de Lisboa.
- Torres, J. E. (2015). *Gestão de Riscos no Planeamento, Execução e Auditoria de Segurança*. Lisboa: Instituto Superior de Ciências Policiais.
- Townshend, C. (2006). *O Terrorismo. Compreender*. Vila Nova de Famalicão: Quasi Edições.
- Tzu, S. (2009). *A Arte a Guerra*. Lisboa: Bertrand Editora.
- Valente, M. M. (2014). Da Segurança Pública: Contributos para uma Tipologia. Em J. B. Gouveia, & R. Pereira, *Estudos de Direito e Segurança. Volume I* (pp. 287-316). Coimbra: Almedina.
- Wagner, A. (2011). Intelligence for Counter-Terrorism: Technology and Methods. *Journal of Policing, Intelligence and Counter Terrorism*, 48-61.

Wheaton, K. J., & Beerbower, M. T. (2006, 5 19). Towards a New Definition of Intelligence. *Stanford Law & Policy Review*, pp. 319-330.

Wheelen, T. L., & Hunger, J. D. (1989). *Strategic Management and Business Policy*. Estados Unidos da América: Addison-Wesley Publishing Company.

Wippl, J. W. (2016). Observations on Successful Espionage. *International Journal of Intelligence and CounterIntelligence*, 585-596.

Zippelius, R. (1997). *Teoria Geral do Estado*. Lisboa: Fundação Calouste Gulbenkian.

DOCUMENTOS

British Army. (2002, 03). Army Field Manual. Part 3 - Intelligence, Suverillance, Target Acquisition and Reconnaissance. Retirada a 25 de abril de 2020, de https://wikileaks.org/wiki/UK_Intelligence,_Surveillance,_Target_Acquisition_and_Recon_ISTAR_handbook_2002

Central Intelligence Agency. (2003, 9 4). Guidelines on Medical and Psychological Support to Detainee Interrogation. Retirado a 15 de abril 2020, de <https://www.cia.gov/library/readingroom/docs/0006541536.pdf>

Department of the Army. (2006, 09). *Army Intelligence and Security Doctrine*. Retirado a 12 de abril de 2020 de Federation of American Scientists: <https://fas.org/irp/doddir/army/fm2-22-3.pdf>

Comission on Organization of the Executive Branch . (1955, 06 29). *Comission Report on Intelligence Activities*. Retirado a 10 de abril de 2020 de Central Intelligence Agency: <https://www.cia.gov/library/readingroom/docs/CIA-RDP86B00269R000100020003-5.pdf>

DeVine, M. E. (2019, 06 14). Covert Action and Clandestine Activities of the Intelligence Comunity: Selected Definitions in Brief. Congressional Research Service. Retirado a 16 de abril de 2020, de <https://fas.org/sgp/crs/intel/R45175.pdf>

Elsa, J. K. (2004, 9 8). Lawfulness of Interrogation Techniques under the Geneva Conventions. (C. R. Service, Ed.) Estados Unidos da América. Retirado a 29 de março de 2020, de <https://file.wikileaks.org/file/crs/RL32567.pdf>

Home Office. (2018, 08). Covert Human Intelligence Sources - Revised Code of Practice. Reino Unido. Retirado a 4 de abril de 2020, de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf

Home Office. (2018, 08). Covert Surveillance and Property Interference. Reino Unido. Retirado a 4 de abril de 2020, de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

Institute for Economics & Peace. (2019, 11). *Global Terrorism Index 2019*. Retirado a 12 de maio de 2020, de Vision of Humanity: <https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2019-web.pdf>

Intelligence and Security Committee of Parliament. (2018, 7 18). *Intelligence and Security Committee of Parliament. Diversity and Inclusion in the UK Intelligence Community*. Retirado a 7 de abril de 2020, de Gov.uk: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/740654/20180718_Report_Diversity_and_Inclusion.pdf

Intelligence and Security Committee of Parliament. (2020, 07 21). Intelligence and Security Committee of Parliament - Annual Report 2018–2019. Retirado de The Cost of Intelligence Sharing and the Value of Transparency: <https://docs.google.com/a/independent.gov.uk/viewer?a=v&pid=sites&srcid=aW5kZXBlbmRlbnQuZ292LnVrfGlzY3xneDo3Zjk2MDBmZjk3NmI0MDg0>

Office of the Director of National Intelligence. (n.d.). National Intelligence Strategy of United States of America. Retirado a 15 de abril de 2020, de https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf~

Williams, H. J., & Blum, I. (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. Santa Mónica: Rand Corporation. Retirado a 10 de março de 2020, de https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf

WEBSITES

BBC. (2019, 11 14). *Las Vegas shooting: At least 59 dead at Mandalay Bay Hotel*. Retirado de BBC: <https://www.bbc.com/news/world-us-canada-41466116>

BBC News. (2020, 09 27). *US intelligence agencies' 'black budget' detailed*. Retirado de BBC New: <https://www.bbc.com/news/world-us-canada-23903310>

British Army. (2020, 04 26). *The British Army. Operations and Deployments*. Retirado de The British Army: <https://www.army.mod.uk/deployments/>

British Army. (2020, 04 26). *Who we are. Intelligence Corps*. Retirado de The British Army: <https://www.army.mod.uk/who-we-are/corps-regiments-and-units/intelligence-corps/>

Carroll, T. P. (2002, 04 14). *The CIA and the War on Terror*. Retirado de Middle East Forum: https://www.meforum.org/meib/articles/0209_me2.htm

Central Intelligence Agency. (2019, 06 6). *Human Intelligence*. Retirado de Central Intelligence Agency: <https://www.cia.gov/offices-of-cia/ clandestine-service/intelligence.html>

Central Intelligence Agency. (2020, 01 11). *CIA Vision, Mission, Ethos & Challenges*. Retirado de Central Intelligence Agency: <https://www.cia.gov/about-cia/cia-vision-mission-values>

Central Intelligence Agency. (2020, 4 10). *INTelligence: Human Intelligence*. Retirado de Central Intelligence Agency: <https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-human-intelligence.html>

CNN. (2019, 11 14). *Orlando shooting: 49 killed, shooter pledged ISIS allegiance*. Retirado de CNN: <https://edition.cnn.com/2016/06/12/us/orlando-nightclub-shooting/index.html>

Comité Internacional da Cruz Vermelha. (2020, 03 28). *As Convenções de Genebra de 1949 e seus Protocolos Adicionais*. Retirado de Comité Internacional da Cruz Vermelha: <https://www.icrc.org/pt/doc/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva->

conventions.htm?gclid=Cj0KCQjw6_vzBRCIARIsAOs54z6P4d6m3AFIKxPgX
kjQr8tgk3tHPDs1-mNK4MmiR21EWANAcCJ9zQaAq9GEALw_wcB

Conselho da União Europeia. (2019, 11 14). *Estratégia antiterrorista da UE*. Retirado de Conselho da União Europeia: <https://www.consilium.europa.eu/pt/policies/fight-against-terrorism/eu-strategy/>

Federal Bureau Investigation. (2020, 05 02). *Intelligence Branch*. Retirado de Federal Bureau Investigation: <https://www.fbi.gov/about/leadership-and-structure/intelligence-branch>

Federal Bureau of Investigation. (2020, 1 4). *What We Investigate*. Retirado de Federal Bureau of Investigation: <https://www.fbi.gov/investigate>

Gov.uk. (2020, 01 04). *About us*. Retirado de Gov.uk: <https://www.gov.uk/government/organisations/national-security/about>

Gov.uk. (2020, 1 4). *Intelligence and security committee*. Retirado de Gov.uk: <https://www.gov.uk/government/groups/intelligence-and-security-committee>

Gov.uk. (2020, 1 4). *National Counter Terrorism Security Office*. Retirado de Gov.uk: <https://www.gov.uk/government/organisations/national-counter-terrorism-security-office>

Intelligence Community. (2020, 01 02). *Mission*. Retirado de INTEL.gov: <https://www.intelligence.gov/mission>

Investigatory Powers Comissioner's Office. (2020, 04 27). *Investigatory Powers Comissioner's Office*. Retirado de <https://www.ipco.org.uk/>

Justice. (2020, 04 27). *Regulation of Investigatory Powers Act 2000*. Retirado de Justice: <https://justice.org.uk/regulation-investigatory-powers-act-2000/>

Legislation.gov.uk. (2020, 04 27). *Intelligence Services Act*. Retirado de Legislation.gov.uk: <http://www.legislation.gov.uk/ukpga/1994/13/contents>

Legislation.gov.uk. (2020, 04 27). *Security Service Act 1989*. Retirado de Legislation.gov.uk: <http://www.legislation.gov.uk/ukpga/1989/5/introduction>

MI5. (2020, 04 17). *Counter-terrorism*. Retirado de MI5: <https://www.mi5.gov.uk/counter-terrorism>

- MI5. (2020, 04 17). *Gathering Intelligence*. Retirado de MI5: <https://www.mi5.gov.uk/gathering-intelligence>
- MI5. (2020, 04 18). *What to Look For*. Retirado de MI5: <https://www.mi5.gov.uk/what-to-look-for>
- MI5. (2020, 04 19). *Agent FAQs*. Retirado de MI5: <https://www.mi5.gov.uk/agent-faqs>
- Nações Unidas. (2019, 11 13). *Maintain International Peace and Security*. Retirado de Nações Unidas: <https://www.un.org/en/sections/what-we-do/maintain-international-peace-and-security/index.html>
- Nações Unidas. (2019, 11 13). *UN Global Counter-Terrorism Strategy*. Retirado de Nações Unidas: <https://www.un.org/counterterrorism/ctitf/un-global-counter-terrorism-strategy>
- NATO. (2019, 11 13). *Countering Terrorism*. Retirado de NATO: https://www.nato.int/cps/en/natohq/topics_77646.htm
- Office of the Director of National Intelligence. (2020, 01 04). *Member of the IC*. Retirado de Office of the Director of National Intelligence: <https://www.dni.gov/index.php/what-we-do/members-of-the-ic#dia>
- Office of the Law and Revision Counsel. (2020, 04 16). United States Code. Retirado de <https://uscode.house.gov/>
- Pringle, R. W. (2019, 12 18). *Central Intelligence Agency*. Retirado de Encyclopaedia Britannica: <https://www.britannica.com/topic/Central-Intelligence-Agency/Activities>
- Roser, M., Nagdy, M., & Ritchie, H. (2018, 02 01). *Terrorism*. Retirado de Our World in Data: <https://ourworldindata.org/terrorism>
- Scientists, F. o. (2020, 09 27). *Intelligence Agency Budgets: Commission Recommends No Release But Releases Them Anyway*. Retirado de Federation of American Scientists: <https://fas.org/irp/commission/budget.htm>
- Skynews. (2019, 11 14). *Britain's year of terror: Timeline of attacks in 2017*. Retirado de Skynews: <https://news.sky.com/story/britains-year-of-terror-timeline-of-attacks-in-2017-11036824>

Soares, F. L. (1975). *Introdução à Política*. Lisboa: Diabril.

START. (2019, 11 13). *About the GTD*. Retirado de START - National Consortium for the Study of Terrorism and Responses to Terrorism: <https://www.start.umd.edu/gtd/about/>

The Guardian. (2019, 11 14). *London bombings: the day the anti-terrorism rules changed*. Retirado de The Guardian: <https://www.theguardian.com/uk/2010/jul/07/london-bombings-anti-terrorism>

Vision of Humanity. (2019, 11 14). *Global Terrorism Index*. Retirado de Vision of Humanity: <http://visionofhumanity.org/indexes/terrorism-index/>

Worldometers. (2019, 11 14). *Countries in the world by population (2019)*. Retirado de Worldometers: <https://www.worldometers.info/world-population/population-by-country/>

ANEXO I

As tabelas que se seguem foram criadas pelo autor da presente dissertação, sendo elaborados com base nos dados disponibilizados pelo *website* “START”, consultável em <https://www.start.umd.edu/research-projects/global-terrorism-database-gtd>.

1. EVOLUÇÃO DO TERRORISMO AO NÍVEL MUNDIAL

| | Atentados | Mortes | Feridos |
|------|-----------|--------|---------|
| 2001 | 1913 | 7735 | 28167 |
| 2002 | 1333 | 4805 | 7162 |
| 2003 | 1278 | 3317 | 7384 |
| 2004 | 1166 | 5743 | 12022 |
| 2005 | 2017 | 6331 | 12734 |
| 2006 | 2758 | 9380 | 15550 |
| 2007 | 3242 | 12824 | 22524 |
| 2008 | 4805 | 4741 | 18998 |
| 2009 | 4722 | 9277 | 19147 |
| 2010 | 4826 | 4822 | 15953 |
| 2011 | 5077 | 8246 | 14659 |
| 2012 | 8529 | 15501 | 25451 |
| 2013 | 12041 | 22273 | 37688 |
| 2014 | 16908 | 44492 | 41130 |
| 2015 | 14977 | 38853 | 44064 |
| 2016 | 13626 | 34858 | 40076 |
| 2017 | 10980 | 26568 | 25066 |
| 2018 | 9607 | 22987 | 20259 |

2. EVOLUÇÃO DO TERRORISMO POR REGIÃO DO MUNDO (ENTRE 2001 E 2018)

| | Atentados | Mortes | Feridos |
|-------------------------------|-----------|--------|---------|
| Oceânia | 91 | 14 | 35 |
| América Central/ Caraíbas | 80 | 55 | 105 |
| Asia Central | 175 | 147 | 266 |
| Asia Oriental | 171 | 798 | 1175 |
| Europa de Leste | 3360 | 4407 | 6709 |
| Médio Oriente/Norte de África | 37996 | 107163 | 161998 |
| América do Norte | 633 | 3564 | 24094 |
| América do Sul | 2339 | 2466 | 4104 |
| Ásia do Sul | 33232 | 70996 | 94223 |
| Sudoeste Asiático | 8942 | 7058 | 13839 |
| África Subsaariana | 13300 | 57125 | 33684 |
| Europa Ocidental | 2702 | 562 | 2936 |

3. EVOLUÇÃO DO TERRORISMO NO REINO UNIDO

| | Atentados | Mortes | Feridos |
|------|-----------|--------|---------|
| 2001 | 94 | 8 | 33 |
| 2002 | 21 | 2 | 13 |
| 2003 | 23 | 2 | 11 |
| 2004 | 5 | 0 | 2 |
| 2005 | 30 | 57 | 787 |
| 2006 | 6 | 0 | 0 |
| 2007 | 20 | 4 | 13 |
| 2008 | 39 | 0 | 8 |
| 2009 | 23 | 3 | 12 |
| 2010 | 57 | 0 | 22 |
| 2011 | 47 | 1 | 3 |
| 2012 | 55 | 2 | 2 |
| 2013 | 137 | 4 | 64 |
| 2014 | 103 | 0 | 4 |
| 2015 | 115 | 1 | 23 |
| 2016 | 104 | 9 | 20 |
| 2017 | 123 | 42 | 301 |
| 2018 | 100 | 2 | 18 |

4. EVOLUÇÃO DO TERRORISMO NOS ESTADOS UNIDOS DA AMÉRICA

| | Atentados | Mortes | Feridos |
|------|-----------|--------|---------|
| 2001 | 47 | 3014 | 21894 |
| 2002 | 33 | 4 | 11 |
| 2003 | 33 | 0 | 0 |
| 2004 | 9 | 0 | 0 |
| 2005 | 21 | 0 | 0 |
| 2006 | 6 | 1 | 14 |
| 2007 | 8 | 1 | 14 |
| 2008 | 18 | 2 | 13 |
| 2009 | 12 | 22 | 50 |
| 2010 | 17 | 4 | 17 |
| 2011 | 10 | 0 | 2 |
| 2012 | 20 | 7 | 7 |
| 2013 | 20 | 23 | 436 |
| 2014 | 28 | 26 | 19 |
| 2015 | 38 | 54 | 58 |
| 2016 | 67 | 68 | 143 |
| 2017 | 66 | 96 | 946 |
| 2018 | 67 | 45 | 61 |

ANEXO II

Estrutura orgânica das disciplinas de pesquisa de informações. Produzido pelo autor da dissertação, com base na bibliografia apresentada.

