Departamento de História

Sistemas de Informações Nacionais.

Contributos para a percepção da eficácia

António Pedro Vieira da Silva Cordeiro de Menezes

Dissertação submetida como requisito parcial para obtenção do grau de

Mestre em História, Defesa e Relações Internacionais

Orientador(a):
Doutor Francisco Miguel Gouveia Pinto Proença Garcia, Professor Agregado,
Academia Militar

Co-orientador(a):
Doutor Heitor Alberto Coelho Barras Romana, Professor Associado,
Instituto Superior de Ciências Sociais e Políticas

Janeiro, 2012

AGRADECIMENTOS

À Ana, minha esposa, e filhos, Carolina e António, que se viram privados da minha presença e da minha atenção deixo, nestas curtas palavras, o meu reconhecimento pela paciência e apoio demonstrado.

RESUMO

Desde tempos imemoráveis que os decisores procuram conhecer o meio que os rodeia de forma a minimizar a incerteza imposta pelo meio de modo a atingirem objectivos ou salvaguardar interesses das comunidades que lideram.

Para atingir tal desiderato, os Estados, possuem meios que lhes permitem lidar de forma racional com as mais diversas situações impostas pelo meio que as rodeia. Emergem, de entre os órgãos dos Estados, os Sistemas de Informações Nacionais (SIN). Têm como fim último, alimentar o processo de decisão coligindo e analisando informação e, assim, identificar correctamente o problema posto ao decisor, cujas decisões são tipicamente caracterizadas pelo risco substancial, pela grande incerteza e pelo valor do que está em jogo para os Estados.

O objectivo da presente dissertação de mestrado é o de identificar como a eficácia de um sistema de informações nacional poderá ser medido. Para isso, procuramos, através de uma análise holística aos sistemas de informações nacionais, cujo enfoque é colocado na *intelligence* enquanto estrutura, conhecimento e actividade, perceber qual a influência da *intelligence* no ciclo de decisão em política externa. O argumento apresentado é o de que a eficácia de um SIN pode ser medida através da maximização relativa das capacidades críticas que influenciam a amplitude do ciclo de decisão, de política externa, do adversário.

Procuramos, então, contribuir com uma percepção de eficácia, de um sistema de informações nacional, de modo a que se atinja a vantagem de decisão e, concomitantemente, o desiderato da eficiência, sem incorrer no perigo de macular o produto e a eficácia de um SIN. O preço de procurar a eficiência sem ter uma noção da eficácia é o de mergulhar os decisores na incerteza.

PALAVRAS-CHAVE: Informações; Sistemas; Eficácia; Política externa

ABSTRACT

Since immemorial eras decision-makers try to know the environment that surround them in order to minimize uncertainty and to achieve goals or safeguarding interests of the community which they are the leaders.

To achieve that objective, states, have means that help them in dealing, in a rational way, with situations imposed by the external environment. In this sense, within the agencies of the state, emerge the National Intelligence Systems (NIS). They have, as an ultimate objective, to feed the decision-making process, collecting and analyzing data. By doing this, they can identify, in a correct manner, the decision problem, posed to decision-makers, whose decisions are typically characterized by the substantial risk, a great uncertainty and by the value of what is in stake.

The objective of the present master's thesis is to identify how the effectiveness of a NIS can be measured. In this sense, we try to, throughout a holistic analysis, with the focus on intelligence as a structure, knowledge, and activity, to understand what the influence of intelligence is in the decision cycle in foreign policy. The presented argument is that the effectiveness of a NIS can be measured through the relative maximization of the critical capabilities that have influence in the amplitude of the decision-making cycle in foreign policy, ours and the opponent.

We hope to contribute with a perception of effectiveness of a NIS, in order to facilitate the advantage of decision and at the same time to achieve the efficiency, without taking risks in endanger the product and the effectiveness of the NIS. The price to find efficiency without an idea of effectiveness is to drive decision-makers to uncertainty.

KEY WORDS: Intelligence; Systems; Effectiveness; Foreign Policy

ÍNDICE

ÍNDICE DE FIGURAS

GLOSSÁRIO DE SIGLAS

AC – Acção Coberta

ADM – Armas de Destruíção Massiva

CI - *Counterintelligence*

CIA – *Central Intelligence Agency*

CMOC – *Civil-Military co-Operation Center*

COMINT – *Communications Intelligence*

DIA – *Defense Intelligence Agency*

DNI – *Director of National Intelligence*

DoD – *Department of Defense*

DoS – *Department of State*

ELINT – *Electronic Intelligence*

EUA – Estados Unidos da América

FISINT – *Foreign Instrumentation Signals Intelligence*

GEN – Grande Estratégia Nacional

GEOINT – *Geographic Intelligence*

GPS - Global Positioning System

GWOT – *Global War On Terrorism*

HUMINT – *Human Intelligence*

IC – *Intelligence Community*

KIQ – *Key Intelligence Question*

MASINT – *Measurement and Signature Intelligence*

MI-5 – British Security Service

MI-6 – British Secret Intelligence Service

NIPF - *National Intelligence Priorities Framework*

NIT – *National Intelligence Topics*

NSC – *National Security Council*

ONG – Organização Não-Governamental

OODA – Observar, Orientar, Decidir e Agir

OSINT – *Open Source Intelligence*

PfP – *Partners for Peace*

RI – Relações Internacionais

SI – Sistema internacional

SIGINT – *Signals Intelligence*

SIN – Sistema de Informações Nacional

TECHINT – *Technological Intelligence*

UK – *United Kingdom*

URSS – União das Repúblicas Socialistas Soviéticas

US – *United States*

USA – *United States of America*

VoIP – *Voice over Internet Protocol*

INTRODUÇÃO

Desde tempos imemoráveis que os decisores procuram conhecer o meio que os rodeia de forma a minimizar a incerteza imposta pelo meio de modo a atingirem objectivos ou salvaguardar interesses das comunidades que lideram.

Para atingir tal desiderato, os Estados, possuem meios que lhes permitem lidar de forma racional com as mais diversas situações impostas pelo meio que as rodeia. Emergem, de entre os órgãos dos Estados, os Sistemas de Informações Nacionais (SIN). Têm como fim último, alimentar o processo de decisão coligindo e analisando informação e, assim, identificar correctamente o problema posto ao decisor, cujas decisões são tipicamente caracterizadas pelo risco substancial, pela grande incerteza e pelo valor do que está em jogo para os Estados. Quando, privado de tais estruturas, o Estado, "... comporta-se como um limpa-chaminés. Fica rodeado de negro, não vê nada à sua volta, fica desorientado" (Shavit, 2010). Nesse sentido, os Estados com melhores capacidades de produção de informações ou maior capacidade de degradação das capacidades de produção de *intelligence*[1] do adversário podem compensar as desvantagens que possuam em armamento, recursos financeiros e meios militares. Fazem-no ao saber como aplicar a pressão diplomática ou a força, de forma eficiente, talhada para a missão e oportunamente (2009: 63).

Justificação do tema

A temática da *intelligence* não é nova para nós. Não é nova pela ligação de anos de carreira militar dedicada a esta temática, seja no âmbito das Forças Nacionais Destacadas, seja no âmbito da docência.

Quando jovem Oficial subalterno contactámos pela primeira vez, a referida temática, durante a prestação de serviço na Repartição de Informações da Brigada de Reacção Rápida, sendo o cerne das funções a análise de *intelligence*. Posteriormente, quando Capitão, ao desempenhar as funções de oficial de Informações de uma Força Nacional Destacada, em Timor, tomámos contacto com as especificidades da pesquisa e da decorrente análise. Ao desempenhar funções de docente, como Oficial Superior, no Instituto de Estudos Superiores Militares, tivemos a incumbência de ministrar o bloco de matéria de Informações Militares aos cursos de Promoção a Oficial Superior e Curso de Estado-Maior, do Exército. Recentemente, em virtude das comemorações do bicentenário das Invasões francesas, foi-nos solicitada a colaboração, com um artigo, na Revista Militar, no qual a problemática desenvolvida foi a da identificação da eficácia do Sistema de Informações que apoiava as forças anglo-lusas, comandadas por Arthur Wellesley, o futuro Duque de Wellington.

[1] Doravante utilizaremos o vocábolo anglo-saxónico *intelligence* para designar as informações, de modo a ser mais facilitado a explanação no decurso da presente dissertação e, assim, evitar a confusão com o plural da palavra informação.

Portanto, se a *intelligence* foi sempre um assunto que mereceu a nossa atenção, a dissertação de mestrado apresentou-se como a grande oportunidade para uma abordagem holística e profunda acerca da eficácia dos Sistemas de Informações Nacionais.

A forma como os Estados empregam os SIN, de modo a obter a vantagem da decisão, não é consensual. Alguns teóricos, como Peter Gill e Mark Phythian (2006) e Sims (2009), explicam através do que designam por informação para decisores, ou seja, informação com origem em qualquer fonte que apoia os líderes na decisão acerca de qual a modalidade a seguir. Outros, como Derrian (1992) ou Scott (2004), definem como guerra por meios silenciosos. Ambas as visões colocam balizas em termos de actuação dos SIN, ainda que de forma diferente. Assim, para os apoiantes da primeira *escola* a perspectiva é a de informar e não de executar política. Enquanto os proponentes da segunda *escola* perspectivam a acção coberta e diplomacia clandestina como actividades dos serviços de *intelligence*.

Na empresa de perceber a relação entre SIN e decisores e da eficácia dos primeiros, Sims (2009), centra a sua abordagem na Teoria das Relações Internacionais (neo-realismo) para evidenciar a *intelligence* como uma faceta inevitável na competição entre Estados, incrementando a qualidade das decisões relativamente aos adversários. A autora vê os SIN enquanto elemento gerador de *Soft Power*[2] dos Estados, denominando a sua teoria como *Adaptive Realism*.

Keegan (2006) aborda historiograficamente a temática da eficácia da *intelligence* na guerra. Apresenta, ao invés de Sims (2009), o argumento de que, independentemente da sua qualidade, a *intelligence* não apresenta um caminho infalível para a vitória.

Outra abordagem é-nos oferecida por Michael Herman (2004). A base da sua análise centra-se nas falhas apresentadas pelos SIN ou sub-sistemas que o compõem. Esta abordagem, embora não consiga oferecer um rácio entre as falhas e os sucessos – que serão mantidos em segredo por questões, óbvias, de segurança – é uma mais-valia como forma de estruturar um sistema de lições aprendidas – de modo a garantir a avaliação e desenvolvimento de procedimentos e estruturas, entre outros) interno num SIN ou nos seus sub-sistemas de *intelligence*, sendo, por isso, difícil de desenvolver ao nível académico.

Parece-nos, então, que o debate acerca da eficácia dos SIN está longe de ter atingido um ponto final. Entendemos, desta forma, que uma dissertação de Mestrado que verse acerca desta temática não só está actual como tem, mais que nunca, pertinência e oportunidade.

Delimitação do tema e metodologia de estudo

"O "decision-making" dos governos apresenta duas dimensões: a concepção e a execução. Em ambas as dimensões é fulcral a existência de informações que facilitem a pilotagem do sistema de governo " (Romana, 2008: 98). Será, dos decisores, aquele que fizer uso de *intelligence* relevante

[2] Para Joseph Nye, *Softpower"*baseia-se na capacidade de determinar a agenda política para influenciar as preferências de outros" (Nye, 2005: 29). Traduz-se na capacidade de sedução e atracção sem recurso à coerção.

oportunamente o que, porventura, desenvolverá um processo de decisão mais célere, rodeado de menor incerteza, colocando-se em posição de vantagem relativamente ao seu oponente.

É, assim, legítimo inferir que a obtenção de vantagem de *intelligence* tem como fito a vantagem na decisão. Assumindo-se que a eficácia de um Sistema de Informações Nacional é o grau que com que um SIN realiza os seus objectivos, é obtida através da superioridade de *intelligence* relativamente a outrem.

Porém, a busca incessante pela eficiência da organização burocrática do Estado induz os governos democráticos a racionalizarem, constantemente, orçamentos colocando os SIN no centro do debate que passa, necessariamente, pela alocação judiciosa dos recursos[3] às tarefas de *intelligence* nacional sem, com isso, incorrer no perigo de tornar o Estado um ente amputado dos seus órgãos de alerta precoce e de monitorização de ameaças à acção governativa. Para que o Estado não seja mutilado nos seus instrumentos de *intelligence* será, então, necessário acautelar as condições que afectam a eficácia dos SIN de modo a que não atinja a condição de cegueira, identificado por Shabtai Shavit.

O presente estudo procura identificar quais os elementos que determinam a eficácia dos SIN de modo a permitir a vantagem de decisão em política externa. Assim, o «tronco» do texto aborda analiticamente de forma holística, o que Michael Warner refere como sendo "…the key to comparative analysis…" (2009a: 12), os três vectores principais propostos por Sherman Kent[4]: o primeiro, a *intelligence* enquanto *estrutura* facilitadora do conhecimento; o segundo, a *intelligence* enquanto *conhecimento* necessário aos decisores; o terceiro, a *intelligence* enquanto *actividade* própria dos Estados.

O primeiro desígnio identifica os SIN enquanto estruturas e a sua inserção na organização burocrática do Estado; o segundo, o conhecimento, centra-se na geração de conhecimento necessário ao decisor no quadro do desenvolvimento do processo de decisão em política externa, de um Estado democrático ocidental, tendo em consideração a alteração de paradigma que o 11 de Setembro de 2001 veio dar a conhecer; relativamente ao terceiro, a actividade, permite a percepção das actividades conduzidas pelos SIN de modo a atingir os seus objectivos primaciais: o alerta precoce e a salvaguarda do segredo.

Dada a amplitude da temática em apreço, tornou-se necessário delimitarmos o objecto de estudo eleito – a *intelligence* – em três vectores. O primeiro vector, o aspecto geográfico, é delimitado aos Estados assumidos como democracias ocidentais, os quais partilham valores – direitos, liberdades e garantias, entre outros – e as necessidades de segurança, que se traduz numa necessidade de *intelligence*, pelo menos semelhante. O segundo vector, decorrente do primeiro, é o âmbito da actuação, a política externa. Assim, se os Estados democráticos assentam na legitimidade conferida

[3] Humanos, materiais e financeiros.
[4] Sherman Kent *apud* (Herman, 2004: 2)

pelo eleitorado numa lógica de garantir direitos, liberdades e garantias é legítimo assumir que o esforço de *intelligence* recaia sobre o exterior. O terceiro vector, o temporal, foi delimitado ao período pós-11 de Setembro, quando se objectivaram as alterações ao paradigma de segurança dos Estados.

Para a consecução do presente trabalho recorremos ao método dedutivo, utilizando a pesquisa bibliográfica e documental para reunir a informação disponível sobre o tema em apreço. As referências bibliográficas disponíveis, que contactámos para estudar a temática da eficácia dos SIN, são relativamente recentes não sendo, por isso, muito abundantes. Contudo, é possível encontrar referências desde o final da II Guerra Mundial, ainda que a incidência maior seja desde a última década do século XX até à actualidade, época em que a profusão de estudos – artigos e livros – é maior. Esta situação encontrará explicação se tivermos em linha de conta o incremento de desafios aos Estados e o consequente ambiente de incerteza na Cena Internacional, provocados pela globalização e pelo fim do paradigma bipolar.

Consequentemente, no âmbito da metodologia, a base de estudo será multidisciplinar, implicando as Relações Internacionais e os Estudos de *Intelligence*.

Com as Relações Internacionais interpretaremos as relações entre Estados e os demais actores, isto é, a politica externa conduzida pelos Estados. Para proceder à análise da política externa dos Estados, apoiamo-nos, então, num autor de referência nacional, o Prof. António Marques Bessa: O Olhar de Leviathan. Bessa define política externa como *"os domínios em que o Estado-actor se manifesta na cena internacional"* (2001: 84). De acordo com o mesmo autor a política externa, de um qualquer Estado, é desenvolvida pelos seus dirigentes e não é arbitrária. Pressupondo a existência de um processo de decisão com vista a assegurar a sobrevivência da unidade política.

Com os Estudos de *Intelligence*, porque ainda não é possível identificar uma teoria de *intelligence*, procederemos à análise holística da *intelligence*. Para isso apoiamo-nos em dois autores de referência: Mark M. Lowenthal: Intelligence. From Secrets to Policy; e Jennifer E. Sims: A Theory of Intelligence and International Politics, dois autores que, de certa forma, se complementam. Para Lowenthal "… intelligence serves and is subservient to policy and that it works best – analytically and operationally – when tied to clearly understood policy goals" (2006: xi). O autor, através da análise das actividades de *intelligence*, procura identificar questões específicas que levam a que as estruturas de *intelligence "…Sometimes works well; sometimes it does not"* (Lowenthal, 2006: xii). Sims, por sua vez, fundamenta a sua análise através do pressuposto que a *intelligence* permite a vantagem de decisão, ao tornar a decisão melhor ou por tornar a do adversário pior. O sucesso não está em garantir a verdade ou a perfeição da informação, está sim em garantir informação suficientemente melhor que permita obter vantagem sobre o adversário.

Objectivo da análise

Já enumerámos, no ponto anterior, as motivações que nos impeliram à escolha de Sistemas de Informações Nacionais como tema para a dissertação de mestrado. A forma como procurámos

desenvolvê-lo e a metodologia de estudo adoptada encerra, a montante uma questão central, que se assume como a base do «edifício» onde se insere o estudo preconizado: *Como se pode medir a eficácia de um SIN, no âmbito da política externa de um Estado?*

Colocada esta grande interrogação surgem quatros questões derivadas, que fundamentam a procura de respostas objectivas para o desafio temático proposto, a sistematizar nas conclusões:

- Qual o papel dos SIN no âmbito do Estado democrático?
- Quais são os elementos que influenciam a *intelligence*?
- Qual a influência que a *intelligence* detém no ciclo de decisão de política externa?
- Quais os factores da eficácia de um Sistema de Informações Nacional?

Lançadas as questões derivadas, decorre a hipótese de trabalho, implicitamente dominante neste estudo, cuja validação será efectuada ao longo do mesmo:

- A eficácia de um SIN pode ser medida através da maximização das características que garantem a geração de conhecimento, por um lado, e que oferecem a negação do conhecimento ao adversário, por outro, relativamente a um sistema de informações nacional adversário.

Índice explicativo

Á introdução segue-se *Sistemas de Informações Nacionais,* onde efectuamos, num primeiro momento uma breve análise do conceito de *intelligence*, de modo a perceber o que são Sistemas de Informações Nacionais. Num segundo momento, debruçamos a nossa análise nas estruturas de forma a perceber qual a razão da existência das mesmas na estrutura burocrática dos Estados. Pretendemos enquadrar as estruturas de *intelligence* enquanto órgãos do Estado, facilitadores do processo da decisão em política externa. Em síntese, falaremos com especial detalhe na necessidade dos Estados possuírem tais estruturas

O segundo capítulo, *O Conhecimento,* centra-se na produção de conhecimento e, necessariamente, na ligação entre decisores e estruturas. Como linhas mestras, analisaremos o ciclo de produção de informações para perceber quais as lacunas do processo gerador de conhecimento, desenhado para o paradigma do *need to know*, poderá ter no paradigma do *need to share*. Num segundo momento, centramo-nos na *intelligence* enquanto conhecimento e nos desfios que se colocam no sentido da transmissão do produto aos decisores.

O terceiro capítulo, *As Funções*, pretende, num primeiro momento, analisar os factores do ambiente interno que afectam a qualidade do produto dos SIN, tendo em consideração as funções de *Pesquisa* e *Análise* de *intelligence*. Procuramos acima de tudo perceber quais os elementos que emergem, bem como, as limitações a que estão sujeitas, em termos de eficácia. Seguidamente, analisados que estão os factores de ordem interna, interessa estudar os factores que o ambiente externo induz no produto dos SIN, percorrendo as funções de *counterintelligence* e *Acção Coberta*, isto é, as actividades que podem incrementar a amplitude do processo de decisão adversário, de forma a degradar a sua capacidade de decisão ou, em última análise, criar a sua disrupção.

A Eficácia é o quarto capítulo. Tendo em conta os indicadores, necessários para que o produto tenha qualidade, identificados nos capítulos anteriores, analisaremos o comportamento da estrutura, conhecimento e actividade, numa perspectiva de *geração de conhecimento* e de *negação,* de forma a objectivar a vantagem na decisão face ao grau de realização dos objectivos daquelas estruturas, isto é, estamos em condições de perceber como objectivar o conceito de eficácia dos SIN, através da relação entre estas características.

Esta dissertação de mestrado, sobre a eficácia dos SIN, termina com a tese constante da *Conclusão*, que justifica o estudo. Aí daremos resposta às questões derivadas, materializaremos a hipótese de trabalho e sistematizaremos as questões que possam surgir e/ou deixadas em «aberto». A questão central *Como se pode medir a eficácia de um SIN, no âmbito da política externa de um Estado?*, será objectivamente respondida.

> *"Nada é mais necessário ao governo de um Estado do que a providência, pois por esse meio pode facilmente prevenir-se muitos males que, uma vez verificados, não se poderia remediar senão com grandes dificuldades."*
>
> Cardeal-duque de Richelieu[5]

CAPÍTULO I – SISTEMAS DE INFORMAÇÕES NACIONAIS

Desde os tempos mais remotos os decisores, quando envoltos em ambientes agónicos, procuram conhecer o meio que os rodeia de forma a mitigar a incerteza imposta e, com isso, aplicar os meios que possuem com a máxima sobriedade, de modo a atingir objectivos ou salvaguardar interesses. Assim, o uso de informação pertinente e oportuna pode significar uma redução significativa da surpresa[6] estratégica. Para isso, emergem das brumas do século XIX os Sistemas de Informações Nacionais que evoluíram de meras estruturas *ad hoc*, criadas para satisfazer as necessidades de príncipes durante o tempo de guerra, para organizações estruturadas de forma permanente (Jackson, 2005: 21-26).

Porém a literatura acerca da temática começa a ter alguma consistência, apenas, a partir da segunda metade do século XX e uma das primeiras abordagens, tendo em vista a perspectiva de análise de sistemas surge, de acordo com Michael Herman (2004: 1-2), em 1949 pela pena de Sherman Kent. Kent faz uma abordagem holística àquele conceito, identificando três elementos: o produto, fazendo referência a um tipo de conhecimento; a estrutura, abordando o tipo de organização que produz o conhecimento; o processo, as actividades conduzidas pela organização.

Posteriormente, seguindo o racional de Kent, Lowenthal (2006: 9) sublinha que a abordagem da análise do conceito de *intelligence* deverá ser efectuada tendo em consideração os mesmos três elementos, acrescentando, relativamente a Kent, alguns dados que permitem uma compreensão mais detalhada da realidade. Nesse sentido, faz sobressair que a *intelligence*: (*i*) enquanto processo - deve ser entendida como os meios pelos quais certos tipos de informação são requeridos e solicitados, coligidos, analisados e disseminados e na forma como certos tipos de acção coberta são concebidos e conduzidos; (*ii*) como produto – o resultado do processo, isto é, o conhecimento e as operações, *per se*; (*iii*) enquanto organização – fazendo referência às unidades que conduzem as várias funções da *intelligence*, ou seja, numa perspectiva de "…entidade social composta de pessoas e de recursos, deliberadamente estruturada e orientada para alcançar um objetivo comum" (Chiavenato, 2004: 23).

Esta abordagem holística do conceito de *intelligence* permite-nos, então, identificar os elementos

[5] Plessis, Armand Jean du (2008). O Testamento político, Lisboa, Circulo de Leitores. (p. 289).

[6] Pode ser entendida como a situação "that governments (decision-makers, military planners, foreign policy analysts) can never be 100 per cent certain about the current and future motives and intentions of those able harm them in a military sense*"* (Williams, 2008: 134).

essenciais para a construção de uma matriz de análise da noção do conceito de *intelligence*: a organização, o conhecimento e o processo.

1.1. A *Intelligence*

Ao falar de *intelligence* com alguma facilidade se identificam, no imediato, estereótipos associados ao secretismo e à espionagem, percepção para que, por certo, muito contribuíram as obras de Ian Fleming ou John Le Carré, entre outros. No entanto, de acordo com Keegan (2006: 4-5), ainda que estas traduzam algum fundo de verdade, a realidade é muito mais abrangente, sendo possível identificar, *ab initio,* a utilização deste conceito[7] sob dois prismas.

No primeiro, numa noção *latu sensu,* assume-se que a *intelligence* é toda a informação pesquisada, organizada ou analisada de forma a satisfazer as necessidades de qualquer decisor, desde que envolto numa empresa de competitividade.

Nesse sentido, Jennifer E. Sims, uma académica das Relações Internacionais (RI) que desempenhou, cumulativamente, várias funções de relevo na área da *intelligence*[8], no Departamento de Estado (DoS) dos Estados Unidos da América (EUA), apresenta a *intelligence* como sendo "…the collection, analysis, and dissemination of information for decision makers engaged in a competitive enterprise" (2009: 62). A autora entende *competitive enterprise* numa perspectiva abrangente que prevê os negócios, a política, o desporto ou outra, importa, apenas, que os objectivos sejam o cerne da competição. O foco desta académica é o produto, cuja finalidade é a de facilitar as tarefas dos decisores, empenhados em competição, de onde sobressai uma percepção de presente. A noção da Doutora Sims, traduz que o conhecimento[9], desenvolvido ao nível académico, num qualquer ensaio, desde que destinada a decisores envolvidos em actividades de competição é *intelligence*.

As observações de Adda Bozeman, citada por Warner, reforçam a perspectiva de Sims quando aquela autora observa que Estado não é a unidade de trabalho decisiva no estudo da *intelligence* "…relevant decision making…emanates increaseingly from scattered, often dissimulated command posts of liberation fronts, terrorist brigades, provisional governments, or international communist

[7] Ao entendermos conceito como uma apresentação ou representação intelectual e abstracta da essência de um objecto, facilmente percebemos que será necessário isolar e apreender, de um objecto concreto, "determinada nota ou conjunto de notas essenciais que o caracterizam ou definem" (Freitas, 1989: 1078) .

[8] Das quais se destacam *Deputy Assistant Secretary of State for Intelligence Coordination* (1994-1998) e *Intelligence Advisor to the Under Secretary for Management and Coordinator for Intelligence Resources and Planning at the US Department of State* (1998-2001).

[9] De acordo com Edward Waltz (2003: 3) há três níveis de abstracção de conhecimento. Os DADOS – observações individuais, medidas e mensagens primitivas do nível mais baixo (os termos informações em bruto – *raw intelligence* – e evidências são utilizados, de forma frequente, para designar elementos de dados. A INFORMAÇÃO – grupos de dados organizados (o processo de organização pode incluir a classificação, a indexação e a ligação de dados de forma a contextualizar os elementos dos dados para subsequente pesquisa e análise). O CONHECIMENTO – a informação uma vez analisada, compreendida e explicada é conhecimento ou estimativa, o produto das informações (a percepção da informação providencia um grau de compreensão dos relacionamentos estáticos ou dinâmicos dos objectos de dados e da capacidade de modelar a estrutura e comportamentos passados desses objectos), o conhecimento inclui conteúdo estático e processos dinâmicos.

parties*"* (2009a: 17-8). Warner atribui àqueles actores a categoria de *soberanias*, onde inclui os Estados-nação, em virtude da possibilidade de usarem a violência, procurar o controlo de populações, recursos e território. Segundo aquele autor, são estas as características que diferenciam as *soberanias* dos restantes actores cuja rivalidade é meramente comercial, financeira ou desportiva (2009a: 18). Porém, o que distancia os actores Estatais, das restantes *soberanias*, é a legitimidade inerente ao Estado[10], por um lado, e o cariz subversivo, inerente aos segundos por outro, para quem a necessidade de *intelligence* passa, em grande parte, por uma necessidade de sobrevivência de organizações clandestinas[11] e não por uma necessidade de prosseguir um determinado interesse nacional[12].

Assim, ao nível dos actores estatais, a *intelligence* possui um significado mais restrito. Está, por norma, associada às RI, à política externa, à defesa, à segurança nacional e, consequentemente, ao segredo e às instituições designadas de serviços de *intelligence* (Herman, 2004: 1). A *intelligence* apresenta-se como um facilitador das escolhas necessárias para atingir os fins últimos do Estado[13].

Seguindo o racional de Herman, o Professor Heitor Romana refere que numa definição alargada, "estas corresponderão ao conhecimento de elementos estáticos e dinâmicos úteis à escolha, regulação, orientação, monitorização e antecipação de medidas e acções consideradas como estruturantes ou axiais para o planeamento da condução da política dos programas governativos" (2008: 98).

De acordo com o mesmo autor, a informação é coligida e tratada ao nível dos gabinetes políticos sendo, após este processo, incorporada no processo da actuação da política corrente. Salientamos a preocupação do autor, em sublinhar a acção governativa, no que concerne à finalidade da *intelligence*, excluindo todo o tipo conhecimento que gravite fora da esfera do Estado.

Num segundo prisma, *stricto sensu*, a *intelligence* deve ser entendida como a pesquisa de *intelligence* sem o consentimento, a cooperação ou o conhecimento dos «alvos», de forma a alimentar as necessidades do Estado, tendo, por isso, o segredo um papel fulcral.

De acordo com Shulsky muita da informação necessária para a decisão dos governos é acedida por

---

[10] "Classicamente, revelam a existência de soberania três direitos dos Estados: jus tractuum, ou direito de celebrar contratos, o jus legationis ou de receber e enviar representantes diplomáticos e o jus belli ou de fazer a guerra*…"* (Miranda, 2002: 189)

[11] Em virtude das actividades que desenvolvem, causam atrição à autoridade do Estado, o que leva a que, por questões de sobrevivência procurem a clandestinidade, levando a que operem, necessariamente, em segredo.

[12] O interesse nacional "diz respeito a directrizes fundamentais que regem a política do Estado relativamente ao seu ambiente externo (…) são um conjunto de diversas e subjectivas preferências que mudam periodicamente em resposta quer ao processo político interno quer do ambiente externo (…) o que parece ressaltar quanto ao interesse nacional é a segurança, ou seja, a sobrevivência do Estado independente na comunidade internacional, a integridade do território, a população intacta, a economia em desenvolvimento e as características culturais próprias*"* (Sousa, 2005: 105).

[13] Marcello Caetano *apud* Lara (2004: 257) refere que à sociedade política são atribuídos, classicamente, os fins de: segurança – para as pessoas e para os valores que constituem a sociedade política; Justiça – como garante da paz entre as pessoas e os grupos sociais através do respeito mútuo e equidade; bem-estar material e espiritual – as pessoas e grupos sociais são importantes para, de uma forma isolada, satisfazer as necessidades de cultura e economia, cabendo ao poder político, em maior ou menor escala, o provimento da satisfação dessas necessidades.

vias informais ou mecanismos não-estruturados – *media*, negociações oficiais, viagens, contactos com académicos, contactos com executivos de negócios e outros – porém, estes, são manifestamente insuficientes se um decisor tiver necessidade de determinado tipo de informação[14] que apenas os mecanismos organizados e estruturados possam facilitar (1995: 17). Para além do mais, é inerente a necessidade de «tratamento especial», sendo o segredo uma característica destes mecanismos. Deve, então, entender-se *intelligence* como segredo ou informação secreta (Shulsky, 1995: 26). Assim, a *intelligence* foca-se numa determinada tipologia de informação, necessária às escolhas dos decisores, carecendo de ser conduzida por mecanismos organizados e estruturados para o efeito.

Nessa perspectiva, para Heitor Romana, académico português, o conceito de *intelligence* é entendido, em sentido restrito, como *"*…um processo de obtenção de conhecimento fundamental à tomada de decisão quanto à salvaguarda dos interesses permanentes ou conjunturais dos Estados, assumindo uma natureza e finalidade ofensiva e defensiva" (2008: 98). Nesta noção, o autor, apresenta-nos a *intelligence* numa perspectiva holística, isto é, enquanto processo, produto e organização. Relativamente ao processo, Romana, introduz, explicitamente, a ideia de conhecimento. Para que tal seja possível é necessário um conjunto de actividades que variam desde a manifestação das necessidades, pelo decisor, até à disseminação ao decisor, induzindo uma necessidade de relação biunívoca entre as organizações e decisores. Este conhecimento é, então, aquele que garantirá o alerta precoce, bem como a constante monitorização das situações que se tornem fundamentais à tomada de decisão, o autor apresenta-nos a ideia das necessidades de futuro, bem como, de presente. Não sendo, então, todo o conhecimento enquadrado nesta noção. Apenas aquele que é fundamental à tomada de decisão relativa ao interesse nacional – permanente ou conjuntural. Deste modo, remete-nos para a organização uma vez que uma das características desta informação e das necessidades decorrentes do processo de decisão é, precisamente, a necessidade de segredo. A este propósito Lowenthal refere que "secrecy does make intelligence unique. That others would keep important information from you, that you need certain types of information and wish to keep your needs secret" (2006: 4). Pelo que, apenas organizações com características próprias permitem atingir este desiderato, são os SIN, da tutela do Estado. Além disso, esta noção permite-nos entender a *intelligence*, quanto à natureza, com uma actuação defensiva e ofensiva, em relação a actores cujos objectivos sejam conflituais ou potencialmente conflituais com os do próprio Estado.

Sistemas de Informações Nacionais transmitem a ideia de como são organizadas, de forma permanente, tratadas e executadas determinadas necessidades de conhecimento secreto, necessário para que os Estados possam perceber e influenciar a incerteza que lhe é colocada pelo meio externo e que escapam ao seu controlo (Warner, 2009a: 24), de forma a facilitar o processo de tomada de decisão, no quadro da política externa. Enquanto organizações são órgãos do poder executivo tendo

[14] Política, militar, económica, social, ambiental, cultural e sanitária, entre outros.

como consumidores os chefes de Estado ou de Governo ou outras autoridades da administração pública, que conduzem as suas actividades[15] em ambientes adversos.

1.2. Das estruturas

A política externa, que Bessa assume como "os domínios em que o Estado-actor se manifesta na área internacional" (2001: 84), é uma inevitabilidade e nenhum Estado pode abdicar dela. A esse propósito, Robert Merle *apud* Bessa sublinhava que a política externa é tão necessária como indispensável. Necessária, para introduzir medidas correctivas no SI, cujas tendências anárquicas são por demais evidentes. Indispensável, no sentido que separa o plano interno do plano externo, sem a qual a identidade colectiva se dissolveria (2001: 72). A necessidade de interagir com outros actores é tão antiga como a existência humana. Para além do mais, é um dos principais pendões do Estado, uma vez que aquele actor procura, no palco internacional, maximizar o seu interesse nacional face aos demais actores, com quem interage, dando corpo à observação de Morgenthau e Thompson que referem que a "international politics, like all politics, is a struggle for power. Whatever the ultimate aims of international politics, power is always the immediate aim" (1985: 31), sendo considerados, por aqueles autores, como objectivos últimos a liberdade, a segurança, a prosperidade ou, simplesmente, o poder.

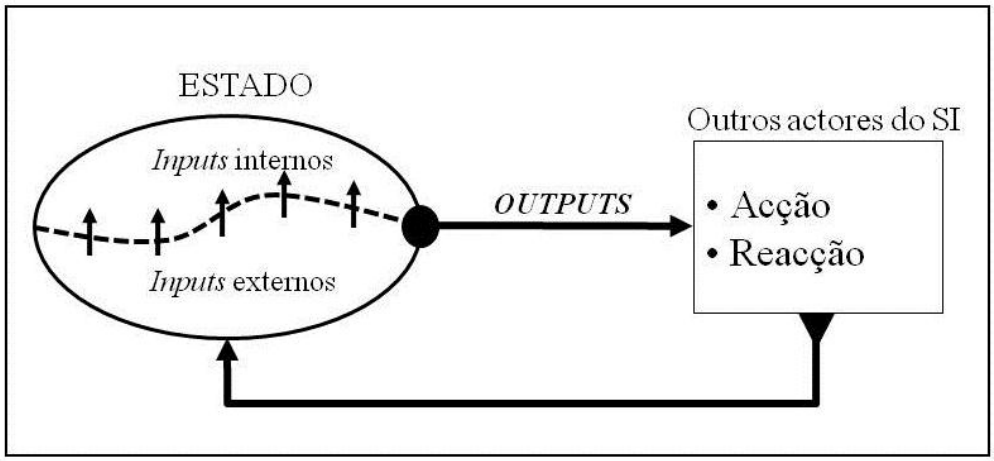

Figura I.1 - Dinâmica da política externa

A política externa (ver figura I.1) poderá, então, ser entendida enquanto actividade de *limes*, na qual se cruza o ambiente externo – o meio onde a mesma se desenvolve – e o ambiente doméstico, do Estado – o enquadramento de base no qual os vectores força são gerados, tendo em vista, segundo Bessa, "certas metas que asseguram, no fundo, a sobrevivência da unidade política em causa" (2001:

[15] Pesquisa, análise, *counterintelligence* e acção-coberta.

86). O que torna bastante onerosos os resultados da decisão que, na concepção de David Easton citado por Dougherty e Pfaltzgraff, "são os outputs do sistema político (…) consistem na distribuição de valores, investida de autoridade, no seio de uma sociedade*"* (2003: 703).

Nesse sentido, a tomada de decisões consiste no acto "de escolher entre opções alternativas que introduzem o problema da incerteza*"* (Dougherty e Pfaltzgraff, 2003: 704), daqueles que, segundo os mesmos autores, actuam em nome do Estado. Porém, de acordo com Max Webber citado por Dougherty e Pfaltzgraff "num estado moderno, o dirigente é inevitávelmente a burocracia, pois o poder não é exercido, nem por discursos parlamentares, nem por enunciados monárquicos, mas sim através da rotina administrativa" (2003: 707). Para além do mais, de acordo com Bessa, para se fazer política externa os políticos "contam com a ajuda de gabinetes de estudo, equipas de especialistas, grupos treinados de informação secreta…" (2001: 121) cujo fito é garantir de forma sistemática uma análise das matérias em apreço. Aquele autor deixa antever que "na ignorância das conjunturas e dos poderes efectivos não é possível tomar decisões acertadas e úteis para a população e até mesmo para o pequeno grupo da elite dirigente" (2001: 121)

Ao sublinhar a necessidade dos Estados possuírem estruturas de *intelligence* permanentes Lowenthal (2006: 2) refere que são quatro as razões principais para que tal suceda: evitar a surpresa estratégica, providenciar experiência de longo prazo, apoiar o processo político e manter o segredo da informação, necessidades e métodos.

O principal objectivo de qualquer organização de *intelligence* será o de manter a monitorização de ameaças[16], eventos e desenvolvimentos, numa perspectiva de segurança nacional[17], isto é, procurar evitar a surpresa estratégica.

Para vários autores, como Colin S. Gray, a questão de evitar a surpresa estratégica não se prende com a surpresa *per se*, que por definição acontece. O problema está nos efeitos nocivos que esta possa produzir ao nível do interesse nacional, uma vez que a "surprise, by definition, is in the hands of our enemies (…) But the the effects of surprise, by and large, are in our hands (…) We cannot aspire to be surprise-proof. We can, however, aim to be proofed against many, perhaps most, of the malign effects of surprise*"* (2005: vi), de modo a que se consigam alocar os meios necessarios de forma atingir a *providência* preconizada pelo Cardeal Richelieu (Plessis, 2008: 289).

Não obstante da grandiosidade do objectivo proposto, muitos Estados têm sido ao longo dos anos

[16] Cabral Couto define ameaça como "…qualquer acontecimento ou acção (em curso ou previsível) que contraria a consecução de um objectivo e que, normalmente, é causador de danos, materiais ou morais. As ameaças podem ser de variada natureza (militar, económica, subversiva, ecológica, etc) (…) Uma ameaça é o produto de uma possibilidade por uma intenção." (1988: 329).

[17] A segurança nacional é definida, pelo Instituto de Defesa Nacional como a "condição da Nação que se traduz pela permanente garantia de sobrevivência em paz e liberdade; assegurando a soberania, independência e unidade, a integridade do território, a salvaguarda colectiva das pessoas e bens e dos valores espirituais, o desenvolvimento normal das tarefas do Estado, a liberdade de acção política dos órgãos de soberania e o pleno funcionamento das instituições democráticas*"* (Carvalho, 2008: 99).

objecto de ataques militares directos cujos efeitos nocivos da surpresa estratégica poderiam afectar, de sobremaneira, a sua sobrevivência. A título de exemplo salientamos o ataque da Alemanha Nazi à União das Repúblicas Socialistas Soviéticas (URSS) – na operação *Barbarossa,* com início a 22 de Junho de 1941 – apesar do pacto Molotov-Ribbentrop[18]; a guerra do Yom Kippur[19], que marca uma ofensiva de surpresa, da coligação Egipto e Síria, ao Estado de Israel, entre 06 e 25 de Outubro de 1973 (Clark, 2004: 1-2) e os atentados de 11 de Setembro de 2001 que, ainda que numa escala limitada em termos de segurança, demonstram o alcance que os efeitos nocivos, da surpresa estratégica, podem alcançar. De facto, de acordo com Alain Bauer e Xavier Raufer (2002), na obra *A Globalização do Terrorismo,* o 11 de Setembro não só afectou, directamente, os EUA, como, de forma indirecta, todo o mundo.

Contudo, para Lowenthal, no quadro da ameaça estratégica, o conhecimento acerca de actividades militares adversárias, que possibilitam ataques de surpresa – ainda que tenha sido a principal razão de existência de estruturas de informações – não é a única tipologia de conhecimento que facilita esta razão. Há outros tipos de *intelligence*, como por exemplo políticas[20], económicas[21] e culturais[22], entre outras, que providenciam *inputs* importantes a analistas e decisores (2006: 6)

Em suma, a função das estruturas de *intelligence* será a de identificar e monitorizar o ambiente externo, de forma a permitir, em tempo, aos decisores alocarem os meios necessários de forma a minimizar os efeitos negativos que a surpresa estratégica possa induzir ao interesse nacional.

A segunda razão apontada por Lowenthal, a garantia de experiência de longo prazo é uma razão cujo impacto no processo de decisão será, porventura, indirecto. É, de alguma forma, a função «educação de líderes» apontada por Michael Handel (2004: 14).

De facto, o ónus da decisão é suportado pelo decisor, porém os apoios a essa decisão chegam através das burocracias. Nesse sentido, em democracia, se comparados com os organismos permanentes, todos os decisores políticos detêm cargos provisórios. A média de permanência do Presidente Norte-americano no poder é de cinco anos (Lowenthal, 2006: 3), e a do Primeiro-ministro português é de quatro anos. Para além do mais, muitos daqueles que servem com estes executivos, em

[18] Assinado secretamente em 1939 e ficava ratificado que ambas as partes acordavam em não ingerir nas esferas de influencia da outra parte. Garantiu fortes relações diplomáticas entre aqueles Estados, apesar da animosidade ideológica.

[19] O mais Santo dos feriados do Judaísmo.

[20] "Pertaining to foreign and domestic policies of governments and the activities of political movements (…) Concerning the dynamics of the internal and external political affairs of foreign countries, regional grouping, multilateral treaty arrangements and organizations, and foreign political movements directed against or affecting established governments or authority*"* (Goldman, 2006: 109)

[21] "The collection and production of foreign intelligence pertaining to the development, production, labor, finance, and taxation of a nation's economic system as well as the distribution and consumption of goods and services" (Goldman, 2006: 47)

[22] "Knowledge resulting from all-source analysis of cultural factors, which assists in anticipating the actions of people or groups of people" (DIA, 2009: 84)

cargos políticos, mantêm-se no cargo por menos tempo ainda, em virtude das reestruturações das equipes governativas – Ministros e Secretários de Estado – operadas durante o período de uma administração ou legislatura.

Outro constrangimento, na acção política, pode ser encontrado no facto de muitos decisores chegarem aos seus gabinetes com uma ampla experiência nos seus campos de actuação sendo, no entanto, muito difícil serem versados em todos os assuntos com que irão lidar (Lowenthal, 2006: 3), de facto "the leader will have to be introduced to the extremely complex world of competing and co-opertating…*"* (Handel, 2004: 15). No sentido de obstar esta situação os decisores terão de cercar-se daqueles cuja experiência e conhecimento em determinadas áreas, como a segurança nacional, é maior. Nesse sentido, porque os quadros das estruturas de *intelligence* tendem a ser mais estáveis que as estruturas de defesa e negócios estrangeiros, particularmente as cúpulas, e porque estas detêm conhecimento e experiência em assuntos relacionados com o interesse nacional é, desta forma, legitimo assumir que a função de garantia de continuidade ou de manutenção da experiência de longo prazo seja efectuada por via das estruturas de *intelligence* (Lowenthal, 2006: 3).

Apoiar o processo de decisão é terceira razão, apontada por Lowenthal, e está intimamente ligada com o *output* do sistema. Assim, de acordo com aquele autor os decisores possuem necessidades constantes de *intelligence* talhada e oportuna que irá garantir o *background*, o contexto, alerta oportuno e a avaliação, relativamente aos riscos, benefícios e prováveis *oucomes* de determinada decisão. Sendo estas necessidades colmatadas pelas estruturas de *intelligence* (Lowenthal, 2006: 4).

Importa que as estruturas mantenham, por um lado, a independência relativamente às escolhas dos decisores, isto é, não produzam *intelligence* de modo a justificar determinadas escolhas, políticas ou *outupts* e, por outro lado, não produzam *intelligence* no sentido de influenciar a escolha para aquela que é da sua preferência (Lowenthal, 2006: 4). Se qualquer uma destas situações ocorrer estamos perante a, designada, politização da *intelligence*. A primeira *top-down* e a segunda, *bottom-up.*

De modo a evitar a situação da politização, deverão ser introduzidos determinados limites na relação entre decisores e estruturas de *intelligence* (Lowenthal, 2006: 4). Primeiro, a ideia que a *intelligence* é distinta da política não que dizer que as estruturas não se preocupem com os *outcomes* da política ou que não o influenciem. Significa, tão-somente, impedir as tentativas a manipulação da *intelligence* de modo a que os decisores efectuem determinada escolha e não influenciar – que é informar – o processo de forma isenta. Segundo, os decisores podem e devem solicitar opiniões às cúpulas das estruturas de *intelligence*. Terceiro, a separação entre decisores e *intelligence* deve funcionar, apenas, num só sentido. A *intelligence* aconselha a política. Nada impede os decisores de preterir a *intelligence* produzida pelas estruturas ou eles próprios introduzir os seus *inputs*[23]. Esta

[23] Uma situação que é vista como sendo diferente da imposição dos seus pontos de vista no produto da *intelligence* (Lowenthal, 2006: 4)

situação também politiza a *intelligence*, o que é algo que quer estruturas, quer decisores procuram evitar (Lowenthal, 2006: 4).

A título de exemplo tomamos como referência a situação que envolveu a *Global War on Terrorism*, mormente nas críticas que argumentavam "that U.S. officials manipulated intelligence to induce the President to overthrow Saddam, and to persuade the public to support the war" (Feith, 2008: ix-x) ou no argumento de Jackson, que refere que a *intelligence* acerca das armas de destruição massiva (ADM) no Iraque foi empregue "…by both American and British governments to strengthen public support for the invasion of Iraq in 2003*"* (Jackson, 2005: 48). Acrescenta, ainda, que a *intelligence* foi usada "as an instrument of policy rather than as a guide for the making of policy" (Jackson, 2005: 48).

Desta discussão de argumentos importa perceber que, para o mesmo efeito, se cruzam as acusações de instrumentalização da *intelligence* por parte das estruturas e, por outro lado, a *intelligence* como uma forma de justificação de uma escolha em política externa.

Por fim, a quarta razão apontada por Lowenthal é a garantia do segredo da informação, necessidades e métodos. Como já foi debatido, é o segredo que torna a *intelligence* única. Lowenthal aponta que as estruturas de *intelligence* apresentam-se como uma necessidade do Estado garantir que determinado tipo de informação se mantém «fora do alcance» de outros agentes ou actores, de que as necessidades de informação são mantidas, com descrição, e que há a garantia de que possui meios de forma a obter a informação necessária ao processo de decisão e à acção política, que outros actores pretendem manter em segredo (Lowenthal, 2006: 4-5).

Parece-nos, então, adequado equacionar os SIN enquanto "…organizações permanentes e actividades especializadas na coleta, análise e disseminação de informações sobre problemas e alvos relevantes para a política externa, a defesa nacional e a garantia da ordem pública de um país" (Cepik, 2003: 85).

1.3. A Organização

O interesse do Estado, desde o fim da guerra-fria, é cada mais afectado por actores cuja indefinição dos contornos impedem a aplicação dos elementos tradicionais de poder. A importância da *intelligence*, enquanto facilitador *do interesse nacional*, é absolutamente primordial. Jorge Silva Carvalho refere que "os serviços de informações constituem, actualmente, a primeira linha da defesa e segurança [do Estado]…" (2006: 92) continua fazendo alusão a que "o puro poder militar já não é suficiente para as combater [ameaças e desafios] com absoluta eficácia, nem mesmo é possível, à maioria dos estados, manter um poder militar efectivamente dissuasor … " (2006: 93). De facto, a «paz longa» marcada pela estratégia da dissuasão nuclear, alimentada pelo medo de uma «vitória de Pirro», que marcava o equilíbrio do sistema, como que de um fiel de balança se tratasse, evoluiu para um sistema internacional caracterizado pela "complexidade, não linearidade, imprevisibilidade, heterogeneidade, mutabilidade e dinamismo*"* (Garcia, 2008: 103).

Os actores transnacionais são, na actualidade, percebidos pelos Estados de forma diferente. Ainda

que não seja um fenómeno novo, a resultante do incremento das solicitações colocadas por estes actores, para além do seu alcance, transformaram os actores não-estatais numa fonte de incerteza internacional. Os grupos terroristas, por exemplo, que antes da queda do muro de Berlim eram um assunto de segurança interna, passaram a desempenhar um papel central a partir do momento que foi identificado, como seu interesse, aterrorizar a população através da violência massiva[24]. Treverton refere que estes actores apresentam ausência de padrões. Classifica a sua acção como circunstancial e insere-os na categoria de mistério, onde a incapacidade de identificar as causas e os efeitos é enorme (2009: 18).

O período pós-guerra fria, em virude das alterações operadas na ordem internacional, veio fazer ressaltar vários problemas ao nivel da organização e gestão dos SIN (Jackson, 2005: 45). Durante a guerra fria as necessidades de *intelligence* sobre o inimigo originou, a Leste e a Oeste, um crescimento massivo das comunidades[25] de *intelligence*, principalmente nos EUA e na URSS, criando cronstangimentos posteriores na construção de um processo de *intelligence* racional e eficaz. Ainda que a maioria dos Estados tenha desenvolvido capacidades de *all-source analysis*, mantiveram-se três factores que atrasaram o processo: o incremento avassalador das actividades de pesquisa[26] patente nas enormes quantidades de dados, sem precedentes, a requerer análise e a proliferação de agências para lidar com este problema; a dificuldade de cooperação e coordenação entre agências foi agravada em virtude da, inevitável, rivalidade burocrática que, como Richard Aldrich *apud* Jackson, observa "each 'national' intelligence community in the west was regularly convulsed by rancorous quarels*"* (2005: 46); e o facto destes Sistemas, desde o fim da Guerra-Fria, terem de lidar com uma série de novos desafios à segurança dos Estados, como por exemplo a proliferação de tecnologia nuclear ou o terrorismo transnacional, entre outros.

Todos estes exemplos demonstram o que Jackson designa como o "essencial element of organization as a limiting factor on effective use of intelligence" (2005: 47), a incapacidade das estruturas se reorganizarem, por norma, de forma preemptiva. Não estando preparadas para fazer face aos novos problemas que se apresentam, ou seja possuirem falta de flexibilidade.

[24] Como no constante dos atentados de 11 de Setembro de 2001, nos EUA, de 11 de Março de 2003, em Espanha, e 07 de Julho de 2005, no Reino Unido

[25] Por comunidade apresentamos o entendimento de Thomas Troy. Para aquele autor a comunidade de *intelligence* é "the colection of those entities loosely knitted together by a number of commitees chaired by the director of Central Intelligence or his appointee. The objective of the knitting is the effective and efficient conduct of the intelligence and counterintelligence functions of the United States government*"* (Troy, 2004: 27). Importa referir que esta noção de comunidade de *intelligence* foi publicada originalmente em 1988, antes da reestruturação que coloca o *Director of National Intelligence*, Norte-americano, com funções de coordenação.

[26] Em virtude da incerteza, por um lado, e do incremento avassalador da informação disponível em fontes abertas e de satélites.

Neste contexto, os Estados, independentemente do regime[27] que possuem, não diferem substancialmente uns dos outros. São hierarquizados e burocráticos procurando garantir os fins de segurança, bem-estar social e justiça, aos seus cidadãos (Treverton, 2009: 15). Para que tal seja possível Michael Mates *apud* Bessa sublinha que "serviços secretos fiáveis é um prerequisito da política: sem uma avaliação objectiva das ameaças ao interesse nacional baseadas em informações seguras de um leque de fontes, os ministros sentirão a falta de uma base sólida para tomar medidas efectivas*"* (2001: 123). Demonstrando da necessidade do Estado possuir estruturas organizadas que permitam, de forma permanente e sistemática, garantir a avaliação objectiva das ameaças ao interesse nacional. Importa, pois, que os SIN possuam uma organização flexivel capaz de fazer face aos desafios actuais, já uma das suas principais características é a de facilmente se adaptarem às situações novas.

Os sistemas de *intelligence*, enquanto estruturas burocráticas, não são instrumentos passivos dos governantes. Ainda que o seu fim último[28] seja o apoio aos decisores em assuntos de segurança nacional (Gookins, 2008: 65-6), a sua actuação tem impacto, de forma directa ou indirecta, nas instituíções e no processo de decisão político. Por outro lado, decisor político também não é um recipiente passivo de *intelligence*, já que influencia todos os aspectos da mesma (Lowenthal, 2006: 2), inclusivamente a organização das estruturas, através das necessidades de informação que possui.

Michael Warner (2009a: 26-37), na senda de identificar quais os factores de que depende o desenho organizacional dos SIN, identifica três vectores base: a «Grande Estratégia Nacional» (GEN), o regime e a tecnologia.

A primeira variável a ter em consideração é a GEN, que segundo Romana deve ser "percebida e desenhada como um sistema. Mas um sistema enquanto forma de organização da decisão e execução política*"* (2008: 99), é o que Loch Johnson sublinha como sendo o ponto de partida para determinar "…the extent of a nation's allocation of scarce resources for intelligence activities is a clear delineation of its international objectives and its adversaries…" (2003: 639). Warner decompõe a GEN em sete elementos: a orientação básica – a postura, que pode ser passiva, agressiva ou vigilante; a geopolítca – que refere as relações de poder relativamente à região e que tem influência na postura; os motivos – são os fins da política externa, que Bessa sistematiza como a segurança, o fim económico, a influência política, a influência cultural e a criação de imagem (2001: 86); os objectivos – relacionados com os motivos, que podem ser a sobrevivência ou o expancionismo, por exemplo; as fontes de apoio ou mediação – as redes de relações de um determinado Estado e podem referir-se a aliados, neutrais, competidores, etc.; situacional – que varia entre o conflito à cooperação; e a cultura estratégica – que é o contexto histórico e a percepção colectiva do mundo e das ameaças que impõe.

[27] Por Regime político pode-se entender "o conjunto das instituições que regulam a luta pelo poder e o seu exercício, bem como a prática dos valores que animam tais instituições" (Levi, 1998: 1081)

[28] É o que "*não está ordenado a fins ulteriores"* (Pires, 1985: 638)

Assim, Estados com menor envolvimento externo ou ameaças podem, por exemplo, descurar a *intelligence* externa[29]. A estratégia também determina alianças e a ligação em *intelligence*, entre estruturas de Estados aliados (Warner, 2009a: 29-9).

O regime político, é a segunda variável.Warner analisa o regime tendo como base cinco elementos: a tipologia de soberania – se é um Estado, um quase-Estado, em império, uma cidade-Estado, etc.; a forma de governo – representativa, aristocracia ou tirania, ou seja, dependendo da forma de governo pode-se perceber a forma de exercer a fiscalização das actividades do SIN; a fiscalização – a forma de exercer a supervisão dos SIN, isto é, seja um governante, conselho de ministros, conselho de fiscalização, ou outros, dependem do tipo de governo; a estrutura ministerial/departamental – o tipo de tarefas e gabinetes criados para conduzir os destinos do Estado podem afectar o sistema que existe para os apoiar, por exemplo, a dependência do sistema pode depender da orgânica do governo; e os desafios internos – alguns os Estados possuem oposição, fricção e, até conflitos internos que pode variar da resistência passiva à insurreição armada e os seus motivos podem ser vários[30] (2009a: 30).

De acordo Bozeman *apud* Warner (2009a: 31), as democracias tendem a dar mais ênfase à *intelligence* externa que à interna, uma vez que, a base da democracia são os direitos, liberdades e garantias dos seus cidadãos. Nesse sentido, para Dziak *apud* Warner (2009a: 31), as ditaduras dão maior preponderância à *intelligence* interna de forma a monitorizar potenciais instigadores contra o poder estabelecido, já que é a manutenção do poder a sua principal preocupação, edificam *counterintelligence States*. Os Estados Imperiais, tendem a empenhar os esforços da *intelligence* quer internamente quer em relação a Estados inimigos ou potencialmente inimigos.

Por fim, a tecnologia, que ao determinar os objectos da *intelligence* e os meios empregues, também produz influência nas estruturas. Assim, Warner identifica cinco elementos, na decomposição desta variável: a informação – a forma como se pesquisa, armazena, transmite e protege a informação; a produção – sugere os «alvos» do sistema, por exemplo, os esforços de *intelligence* direccionados a uma sociedade rebelde, baseada no trabalho «escravo», serão diferentes se o «alvo» for uma sociedade desenvolvida tecnologicamente; os recursos – disponíveis aos esforços das *intelligence*, por exemplo, energia, capital humano, etc.; as formas sociais e institucionais – a forma como a sociedade se organiza, isto é, de forma tribal, ou outras, marcam as diferenças das capacidades e necessidades de *intelligence*; militar – a forma como o Estado aplica a violência, a organização, mobilidade, letalidade, etc., determinam as necessidades de oportunidade e relevância da *intelligence*, as capacidades analíticas e possivelmente a importância relativa dos meios de pesquisa e disseminação da *intelligence* produzida por meios humanos ou técnicos.

[29] Lowenthal (2006: 12) refere que foi a ausência de interesses nacionais, para além das suas fronteiras, o factor preponderante para que os EUA se mantivessem, por cerca de 170 sem um SIN organizado.

[30]Diferenças de classe, credo, raça, étnicas ou ideologia, entre outras. Por exemplo, a oposição interna pode ser espontânea, isto é, «nascido» internamente ou com base externa, uma estratégia indirecta de um outro Estado.

O factor tecnológico é, naturalmente, mais sentido por aqueles Estados que procuram manter um elevado nível tecnológico, seja por razões defensivas, seja por razões ofensivas.

Para Michael Herman (2004: 4-5), o desenho organizacional difere entre regiões, porém não por questões idiossincráticas mas por causa de uma história e valores sociais partilhados. Ideia que Lowenthal deixa transparecer quando refere que "U.S. intelligence system remains the largest and most influential in the World*"* (2006: 11), em virtude de ser entendido como um modelo a seguir, um modelo rival ou, apenas, como «alvo». Herman parte da observação de características organizacionais e operacionais dos sistemas americano e britânico, para de seguida explicitar que os padrões se aplicam, aos diversos sistemas nacionais, através de círculos concêntricos. Assim, o núcleo é formado por EUA e Reino Unido, onde os padrões são mais intensos. Num segundo círculo, os sistemas pertencentes aos Estados da Europa Ocidental e Israel, que por possuírem uma história partilhada com os primeiros, as alianças da II Guerra Mundial, as relações militares sobre os auspícios da Organização do Tratado do Atlântico Norte (OTAN) e outros tipos de cooperação internacional, permitem possuir padrões do núcleo, "the most of generalizations offered here apply in some degree to this Western Circle*"* (Herman, 2004: 5). Por fim, o círculo exterior onde se encontram os Estados comunistas e ex-comunistas onde os padrões e generalizações de Herman se fazem sentir de forma bastante ténue.

Para Lowenthal os SIN, ou *intelligence community*, são constituídos, em termos de macro-estrutura, por duas áreas funcionais: a gestão e a execução. A primeira, cobre os requisitos, recursos, pesquisa e produção. A segunda, abrange tarefas como o desenvolvimento dos sistemas de pesquisa, pesquisa e produção de *intelligence* e a manutenção da infraestrutura de apoio. Contudo, aquele autor acrescenta ainda que há outra função, que não sendo das mais fortes ela terá existir, a avaliação, cuja tarefa será de relacionar os meios – recursos: financeiros e humanos – aos fins da *intelligence* – resultados: análises e operações – o que de alguma forma poderá garantir a necessária avaliação interna que suporte a flexibilização necessária para as pressões que o meio coloca nas organizações de *intelligence* (2006: 33-34).

Cepik (2003: 125-128) refere que, ainda que todos os sistemas de *intelligence* possuam as mesmas atribuições, diferem entre si, em termos de desenho organizacional, em virtude da forma como as escolhas estruturais, os diferentes interesses e preferências dos actores relevantes e o ambiente externo influenciam sete elementos: (*i*) o organismo de coordenação das actividades de *intelligence*; (*ii*) as agências ou organizações dedicadas à pesquisa de *intelligence* – em que, de acordo com aquele autor, as agências dedicadas à pesquisa de *Human Intelligence* (HUMINT) estão separadas das agências de *Comunications Intelligence* (COMINT) ou *Electronic Intelligence* (ELINT), por exemplo; (*iii*) as agências de análise; (*iv*) as unidades departamentais de análise das diversas agências; (*v*) os subsistemas de *intelligence* de defesa e segurança; (*vi*) os órgãos de formação e treino; (*vii*) instâncias de fiscalização externa, seja dependente do poder executivo, legislativo ou judicial.

Tendo como base algumas variáveis genéricas – tais como o grau de centralização da autoridade sobre o sistema, o grau de integração analítica da *intelligence*, a maior ou menor separação entre as

funções de *intelligence* e de *policymaking* e a eficácia dos elementos de supervisão externa – o autor identifica três tipologias base dos Sistemas de Informações Nacionais. O primeiro, o modelo «anglo-saxónico»[31], é caracterizado pela grande centralização das unidades do sistema, grau elevado de integração analítica, uma separação média entre *intelligence* e política e uma eficácia média nos mecanismos de supervisão. O segundo, designa como modelo «europeu continental»[32], caracteriza-se como exercendo um grau de autoridade médio sobre as unidades do sistema, uma integração analítica média dos produtos da *intelligence*, um alto envolvimento das actividades de *intelligence* e as instâncias da decisão e, finalmente, uma eficácia baixa nos mecanismos de supervisão das actividades de *intelligence*. O terceiro e último modelo apresentado por Cepik, é aquele que o autor classifica como o modelo «asiático»[33], tem como características principais a baixa centralização da autoridade sobre as unidades do sistema, a alta integração analítica dos produtos de *intelligence*, um envolvimento médio entre as actividades de *intelligence* e as instâncias decisoras e uma eficácia muito baixa dos mecanismos de supervisão.

Em suma, os SIN, enquanto organização, são o resultado de prcessos específicos de criação de soluções para os desafios na àrea do interesse nacional. Contudo, como observam Berkowitz e Allan, citados por Komensky e Burlin, "the intelligence community is a classic burocracy, characterized by centralized planning, routinized operations, and a hierarchical chain of command. All of these features leave the intelligence ill suited for the information age*"* (2004: 126).

Nesse sentido, é permissível inferir que a estrutura, burocrática[34], da comunidade de *intelligence* teve uma boa prestação enquanto o inimigo que perseguia era também uma burocracia[35]. Na actualidade procurar identificar intenções e movimentações de actores não-estatais – como redes terroristas, de crime organizado ou de proliferação de ADM, ou tecnologia associada – torna-se uma tarefa muito mais complexa. As características erráticas que possuem permite-lhes desafiar a necessidade de segredo e afrontar a cultura que reforça a compartimentação e isola os analistas e agências entre si (Kamensky e Burlin, 2004: 127), observa-se à alteração do paradigma do *need to know* – o segredo e compartimentação – para o paradigma do *need to share* – partilha de *intelligence* – o que vai induzir à necessidade de desenhos organizacionais mais ágeis e com capacidade de adaptação constante ao meio exterior, isto é, mais flexiveis.

A este propósito Amy Zegart *apud* Lewis (2003: 8) observa que pela sua natureza, as burocracias na àrea da segurança nacional, tendem a ser criadas pelo poder executivo e o seu desenho

[31] Inclui os EUA, o Reino Unido, Canadá, Austrália, Nova Zelândia e com algumas reservas a India e a África do Sul.

[32] Inclui a Alemanha, a França, a Federação Russa, a Polónia e a Itália. Inclui, ainda com algumas reservas o Brasil e a Argentina.

[33] O autor inclui Estados como a China, o Japão, a Coreia do Sul, a Coreia do Norte, o Taiwan e com reservas a Indonésia e o Vietname.

[34] Avessa à mudança, por definição (Chiavenato, 2004: 269-270)

[35] O Estado, o que apesar do segredo permitia vaticinar as intenções e movimentações de tal adversário.

organizacional reflece as disputas entre burocracias de segurança nacional. Para além do mais, para Zagart, citada por Cepick (2003: 136), as escolhas estruturais na eclosão do órgão são propensas a perdurar no tempo. A sua alteração efectua-se em virtude dos interesses do poder executivo e do ambiente externo e tenderá a ser lenta, se não for entendida enquanto uma prioridade do poder executivo. Assim, de acordo a mesma autora, os governantes estão sujeitos a constrangimentos de tempo, de conhecimento e controle das suas agendas e da necessidade de realização dos objectivos políticos. A necessidade de obter o apoio da opinião pública não pode ser posto em causa com disputas acerca do desenho organizacional de uma burocracia, uma vez que os subsistemas de *intelligence* têm conhecimento de áreas vitais do Estado, agendas mais delimitadas dos governantes e fortes incentivos para uma participação activa no desenho organizacional. Para além do mais, em sistemas complexos e com dependências cruzadas, com é o caso da maioria dos SIN, os problemas de coordenação são outro dos factores que limita severamente a capacidade de resposta a outros utilizadores que não aqueles que estão na cadeia hierárquica, directa.

Francis Rourke *apud* Dougherty e Pfaltzgraff ao identificar a lei da inércia burocrática referia que "as burocracias imóveis tendem a permanecer imóveis e as burocracias activas tendem a reproduzir actividade" (2003: 708), deixando antever que as burocracias não são todas iguais já que umas apresentam uma maior resistência à mudança do que outras, ainda que para os decisores as burocracias em cujos departamentos executivos forem estimulados a desenvolver determinadas capacidades podem representar algum risco, isto é "quando as burocracias ganham importância, são muito difíceis de refrear*"* (Dougherty e Pfaltzgraff, 2003: 709), uma vez que possuem a capacidade de infuenciar o curso dos acontecimentos. O seu poder depende da vontade do executivo, o governo.

> *"Many intelligence reports in war are contradictory; even more are false, and most are uncertain. What one can reasonably ask of an officer is that he should possess a standard of judgment, which he can gain only from knowledge of man and affairs and from common sense."*
>
> Carl von Clausewitz[36]

CAPÍTULO II – O CONHECIMENTO

Outra forma de equacionar a *intelligence* é enquanto processo, pelo qual determinados tipos de informação são requeridos[37], coligidos, analisados e disseminados, bem como, determinados tipos de acções cobertas são concebidas e conduzidas. Contudo, uma vez que a *counterintelligence* e a acção coberta serão debatidas no capítulo quatro, o presente capítulo centra-se no processo de geração do conhecimento e no produto desse processo, o conhecimento.

Este processo designado, metaforicamente, como «ciclo de produção de informações» procura espelhar um processo cíclico que envolve um conjunto de etapas, repetidos e interdependentes, cujo objectivo será o de adicionar valor-acrescentado[38] aos *inputs* iniciais de modo a obter um produto substancialmente transformado e talhado às necessidades dos decisores. O ciclo de produção de informações operacionaliza "*the process of the discovery of secrets by secret means*" (Waltz, 2003: 2). Isto é, poderá ser entendido como o processo de gerar conhecimento necessário para alimentar o processo de decisão, processando os dados, de forma sistemática de modo a gerar o conhecimento necessário aos decisores

Porém, o referido ciclo não é consensual no que respeita às etapas que o compõem, principalmente relativamente ao papel dos decisores no ciclo, nem no que concerne às suas interdependências, pelo que o modelo do ciclo de produção de informações apresenta várias críticas de onde sobressai a falta de comunicação entre SIN e decisores e entre os actores do processo, principalmente entre a pesquisa e a análise.

2.1. O ciclo de produção de informações

Uma das principais razões pelas quais o ciclo de produção de informações se encontra sistematizado desta forma é explicada por Clark quando refere que "is used because it fits a

[36] Clausewitz, Carl von (1989). On War, Princeton, Princeton University Press. (p. 117).

[37] Por identificar requesitos significifica, para Mark Lownthal, "defining those policy issues or areas which intelligence is expected to make a contribution, as well as decisions as to which of these issues has priorities over others*"* (2006: 54).

[38] Amanda J. Gookins, a este propósito, sublinha que "the intelligence anayst turns information into intelligence by connecting data to issues of national security, thereby giving them value" (2008: 66)

conventional paradigm for problem solving" (2004: 16), o que é reforçado pelo *Defense Intelligence Agency* (DIA) quando se refere ao ciclo de produção de informações como o "... process of developing raw information into finished intelligence for consumers to use in decision-making and action" (DIA, 2009: 17). Isto é, com estas cinco etapas procura-se, de uma forma linear e ordeira, trabalhar o «problema» da *intelligence* desde a questão – o problema – até à resposta – a solução.

2.1.1. O ciclo clássico

O ciclo tem início com os requisitos efectuados pelo decisor[39], percorrendo as seguintes fases: a direcção e planeamento, a pesquisa, o processamento, a análise e produção e a disseminação (conforme a figura II.1).

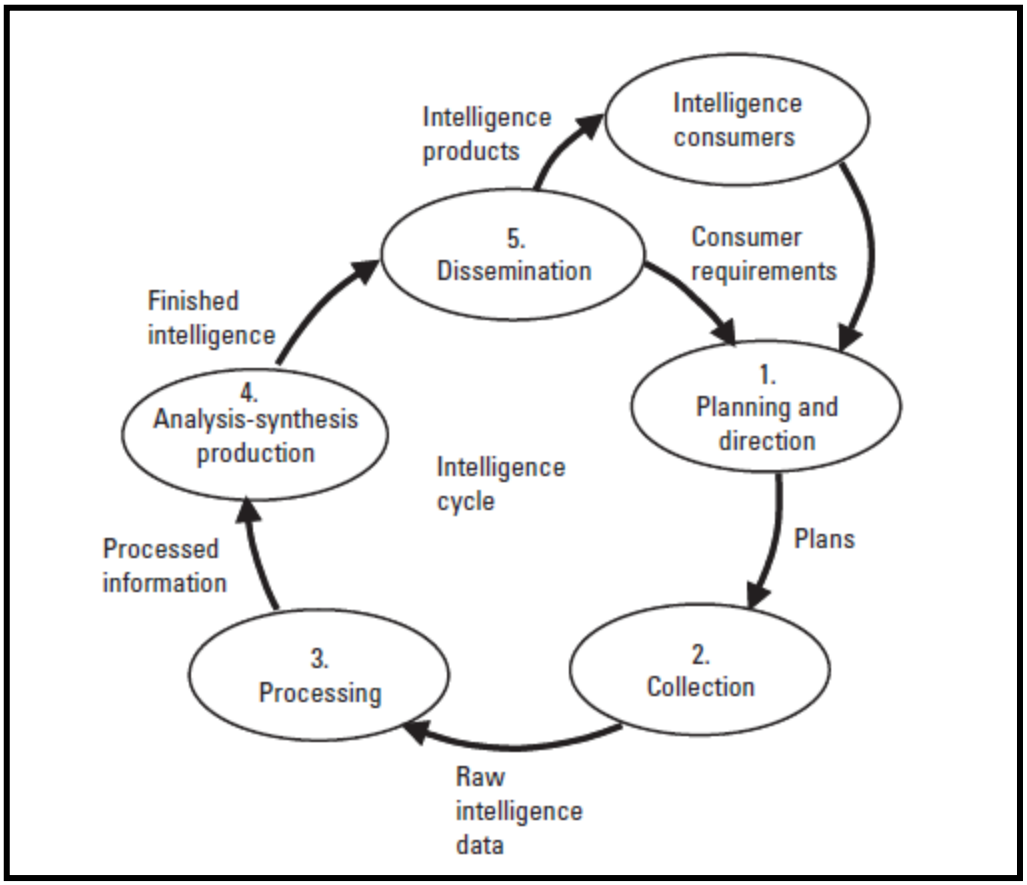

Figura II.1 – Ciclo de Produção de Informações (Waltz, 2003: 34)

A primeira fase, direcção e planeamento, é a fase que dá início ao processo. Esta fase inicia-se com a definição das necessidades, efectuada pelos consumidores, em termos de conhecimento necessário para alimentar o processo de decisão. Os pedidos são dissecados em informação requerida e prioritizados, após o que se procura ter uma percepção dos dados a coligir para estimar ou inferir as respostas solicitadas. As necessidades de dados são usadas como base do estabelecimento dos planos

[39] O utilizador da organização em questão.

de pesquisa que contêm os elementos acerca dos dados a ser recolhidos e dos «alvos»[40], sobre os quais os dados podem ser obtidos (Waltz, 2003: 33). Nesta fase a interacção entre decisores e *intelligence* faz-se através da manifestação das necessidades dos primeiros.

A segunda fase, a pesquisa, decorre da primeira e tem como principal objectivo a recolha dos dados que alimentam o processo. Para o efeito, seguindo o plano traçado na fase anterior, é atribuída, a fontes humanas ou técnicas, a incumbência de recolher os dados requeridos (Waltz, 2003: 33). Nesta fase do processo a interacção com os decisores pode ser feita pelo facto de que "consumers have a wealth of scientific and substantive expertise and information that they can share with the IC [Intelligence Community]" (DIA, 2009: 17). Por norma esta fase compreende uma quantidade de fontes e métodos frágeis[41] que deverão ser «alvo» de protecção.

De acordo com o *Office of the Director of National Intelligence*, nesta fase são usadas seis fontes principais: o *Signals Intelligence* (SIGINT) – a intercepção de comunicações entre pessoas, máquinas ou ambos (de acordo com o Defense Intelligence Agency (DIA, 2009: 12) inclui o COMINT, ELINT e *foreign instrumentation signals intelligence*; o *Imagery Intelligence* (IMINT) – representações de objectos reproduzidos electronicamente ou por meios ópticos em filmes, dispositivos electrónicos ou outro tipo de *media* (pode derivar de fotografias, sensores de radar, sensores de infra-vermelhos, laser e elecctro-ópticos); o *Measurement and Signature Intelligence* (MASINT) – informação tecnológica e científica usada para localisar, identificar ou descrever características de «alvos» específicos – emprega um grupo de disciplinas que engloba o nuclear, a óptica, a rádio-frequência, a acústica, o sísmico e outras – pode identificar, por exemplo, diferentes assinaturas de radar criadas por sistemas aéreos ou a composição química de amostras de ar ou água; a HUMINT – o método mais antigo de recolher informação, é informação que deriva de fontes humanas – a recolha de informação inclui aquisição clandestina – de fotografias, documentos e outro material; recolha aberta – por pessoal diplomático e postos consulares; *debreefing* a nacionais estrangeiros e cidadão nacionais que viagem pelo estrangeiro; contactos oficiais com governos estrangeiros; a *Open-Source Intelligence* (OSINT) – informação disponível ao público sob a forma de material impresso ou electrónico (inclui rádio, televisão, jornais, internet, bases-de-dados comerciais, vídeos, gráficos ou pinturas); a *Geospatial Intelligence* – dados recolhidos de imagens e mapas produzidos pela integração de imagem, IMINT e informação geoespacial – é tipicamente recolhida de satélites comerciais, satélites governamentais, aeronaves de reconhecimento ou por outros meios como mapas, bases-de-dados comerciais, informação de recenseamento, *Global Positioning System*, esquemas utilitários ou outros dados discretos que possuam localizações geográficas (DNI, 2011).

[40] Pessoas, locais ou objectos.

[41] Por frágil entende-se a potencial perda de valor se revelado ao objecto da acção de pesquisa. De acordo com Waltz até os sensores e métodos mais sofisticados podem ser facilmente derrotados, isto é, incapacitados de cumprir a sua missão pela decepção ou negação de acesso (2003: 34).

O processamento dos dados recolhidos constitui a terceira fase do ciclo. Nesta fase os dados são traduzidos, desencriptados, indexados e organizados em bases-de-dados de informação. Esta fase permite verificar se os requisitos do plano de pesquisa estão em consonância com o desejado, o que facilita a tarefa de redefinir os requisitos, se for caso disso, tendo como base os dados recebidos (Waltz, 2003: 34). Nesta fase "policy organizations have robust processing capabilities that can augment the IC's efforts" (DIA, 2009: 18).

Decorrente da anterior surge a fase da análise e produção, a quarta no processo. A informação organizada, na fase anterior, é processada usando técnicas de estimativa ou inferência – através do raciocínio – que combinam os dados, originários de vários sensores, na perspectiva de dar resposta às questões colocadas na primeira fase. Os dados são analisados – fragmentados nas suas componentes e estudados – e as soluções são sintetizadas – construção através da acumulação de evidências. Os tópicos ou assuntos de estudo são modelados e, se for caso disso, surgem novos pedidos de informação, para a pesquisa, e novo processamento poderá ter de ser efectuado de forma a obter dados suficientes, de modo a obter um grau de compreensão aceitável para permitir dar resposta às questões colocadas pelo consumidor (Waltz, 2003: 34-35). O nível político pode interagir incrementando as capacidades da *intelligence*, nesta fase já que "Policy organizations typically have analytic capabilities for their own internal needs, as well as subject matter experts who have specialized knowledge not typically found in the IC*"* (DIA, 2009: 18).

Por fim, a disseminação, onde é expectável o produto ser difundido aos consumidores. Nesta fase, as respostas às questões, colocadas pelos consumidores, são elaboradas em vários formatos, desde imagens dinâmicas de sistemas – de armas ou outros – até aos relatórios formais (Waltz, 2003: 35). Os relatórios formais, em virtude do foco no «horizonte temporal» podem ser categorizados em: *current intelligence repports* – descrevem eventos recentes; *basic intelligence repports* – providenciam uma completa descrição de uma situação específica – e.g. uma ordem de batalha ou uma situação política em determinada região; *intelligence estimates* – nos quais se procura cenarizar tendo por base uma situação actual, isto é, estimar a probabilidade de *outcomes* futuros, constrangimentos e possíveis influências (Shulsky e Schmitt, 2002: 57-61).

2.1.2. As críticas

A sistematização apontada no ciclo de produção de informações procura, fazer transparecer de forma simples, um padrão de raciocínio tendo como base a resolução de problemas, contudo várias têm sido as críticas a este modelo. Seja por via do mundo académico ou da comunidade de *intelligence*, em virtude do desajuste entre o modelo e a realidade.

A razão de ser do processo é a de explicar como se atinge o produto. Sendo o produto dos SIN o conhecimento desenvolvido para apoiar a decisão e as operações conduzidas para garantir o segredo das diversas actividades – necessárias à geração do conhecimento – bem como de apoio à política externa, as críticas recaem, após uma análise detalhada do modelo, no facto do processo que gera o

conhecimento fazer emergir várias questões que produzem impacto quer na qualidade e importância do conhecimento para a decisão – a pertinência – quer na celeridade que o conhecimento é colocado à disposição do decisor – oportunidade. A tónica recai, principalmente, na falta de comunicação entre o sistema e decisores e entre participantes do sistema.

A primeira crítica recai sobre a primeira etapa, em que a noção de que os consumidores de *intelligence* oferecem orientações para dar início ao processo é incorrecto. "Policy consumers do sometimes indicate the main concerns (…) but often they assume that the intelligence system will alert them (…) or provide judgments about the future*"* (Hulnick, 2006: 659). O que significa que serão poucas as situações em que os decisores expressam os requisitos de *intelligence* ao sistema. Esta ausência de comunicação, entre decisores e sistemas, produz um impacto nocivo ao processo de geração de conhecimento. Por variadas vezes os sistemas deparam-se com uma de duas situações: a ausência de orientações, através dos requisitos de *intelligence* e a ausência da definição de prioridades por parte dos decisores. Se a primeira pode dar origem a acusações de intromissão do sistema no domínio da política – politização *bottom up* – o que pode afectar a credibilidade do sistema, a segunda, ao ser ultrapassada pelo sistema – tendo como base as últimas prioridades estabelecidas – pode causar o dispêndio de recursos em áreas sem real prioridade para o consumidor.

Segundo Lowenthal "requirements are not abstract concepts. They are the policy makers agenda" (2006: 180). Todos os decisores possuem determinadas áreas nas quais se devem concentrar, outras onde se gostariam de concentrar e outras, ainda, onde não têm qualquer tipo de interesse mas que requerem a sua atenção ocasional ou regularmente. Todavia, essas orientações nem sempre são fornecidas, o que leva o sistema a procurar guias para a sua acção internamente, já que os gestores da informação do sistema "…often know what gaps exist in the intelligence data base derived from intelligence collectors and analysts" (Hulnick, 2006: 960). Uma evidência que reforça esta observação está naquilo que aquele autor observou nos EUA, durante a administração Carter. Durante esse período foi criado um sistema que formalizava as orientações políticas a fornecer ao sistema. Era composto pelos *National Intelligence Topics* (NIT) que mais tarde passaram a designar-se por *Key Intelligence Question* (KIQ). No caso de não ser dadas orientações via NIT ou KIQ, então o sistema fazia chegar aos decisores uma lista de prioridades de forma a ser sancionada ou alterada de acordo com as necessidades da agenda política. Porém, nenhum dos métodos funcionou em pleno (2006: 960). Mais recentemente, durante a administração Bush, em 2003, foi criado o *National Intelligence Priorities Framework* (NIPF), cujas prioridades são revistas, semestralmente, pelo Presidente e pelo *National Security Council* (NSC). Este sistema pretende agilizar o processo estando ligado, directamente, aos recursos de análise e pesquisa, para garantir que as necessidades mais urgentes são cobertas e que os vazios de informação são preenchidos no imediato.

O racional inerente ao NIPF é o de permitir flexibilizar e agilizar o processo de prioritização das necessidades, enquanto ligação formal entre decisores e sistema. Porém, ainda que as intenções, associadas à sua implementação, sejam boas o sistema apresenta falhas. Primeiro, porque nenhum

requisito começa a ganhar visibilidade enquanto não estiver identificado como de alta prioridade. Em segundo lugar, porque decorrentes da natureza volátil das relações internacionais surgem, sem qualquer tipo de aviso, muitos requisitos designados de *ad hoc*, cuja prioridade é elevada. E, em terceiro lugar, as revisões de prioridades nem são sempre efectuadas, de acordo com os *timings* previstos, originando a que se mantenham activos requisitos obsoletos tornando o sistema estático (Lowenthal, 2006: 56-59).

Mesmo com o NIPF os requisitos têm muitas vezes origem no interior do próprio sistema ou "…driven by world events" (Hulnick, 2006: 960), levando a que o sistema se concentre em determinadas áreas, em detrimento de outras, uma vez que os recursos que dispõe são escassos e não permitem uma cobertura global (Lowenthal, 2006: 180), correndo o perigo de não eliminar o vazio de informação, por poder alocar os recursos de forma desadequada às necessidades do decisor. Sendo o vazio de informação acerca das ADM no Iraque um bom exemplo (Risen, 2006: 90).

Na segunda etapa, a pesquisa, também é possível identificar desajustes entre a realidade e o ciclo de produção de informações. A noção que a pesquisa tem inicio a partir do momento que se identifica o vazio de conhecimento é, também, incorrecto.

Na maioria das vezes, quando se identificam as necessidades ou vazios de conhecimento as operações de pesquisa já se encontram a decorrer. Por exemplo, de acordo com Hulnik (2006: 960-961) uma operação de HUMINT, poderá necessitar de um tempo alargado para encontrar e recrutar a pessoa que tem acesso à informação desejada. Se a pesquisa não tiver a capacidade de antecipar o «alvo», com base nos vazios de informação, provavelmente quando se tiver acesso à pessoa certa a informação será inoportuna. Para além do mais, no que concerne à OSINT, há necessidade de planear, *a priori*, a pesquisa dos dados de fontes abertas de forma a garantir o acesso ao material necessário. Uma vez que a quantidade de dados disponíveis é de tal forma avassalador – disponíveis na internet, em jornais ou outros – torna-se difícil, na actualidade, produzir *intelligence* relevante e oportuna somente após a manifestação das necessidades de *intelligence*. A IMINT, cujos satélites são os seus principais sensores, também não é o suficientemente flexível de forma a poder redireccionar, oportunamente, o foco das suas actividades de pesquisa sempre que a situação o exige. Nesse sentido, Hulnik (2006: 960) observa que durante o conflito das Malvinas, os EUA não puderam apoiar os britânicos com imagens de satélite porque aquela plataforma, que estava programada para vigiar a URSS, passava à vertical das Malvinas, apenas, de noite.

Na terceira etapa, a análise, os desajustes com a realidade são variados, no entanto a principal causa é a falta de comunicação com a pesquisa. E a ideia que a pesquisa alimenta a análise é, na realidade, de alguma forma distorcida.

Primeiro, porque "analysts do not always need new intelligence material to understand world events*"* (Hulnick, 2006: 961). Na realidade as bases-de-dados da análise possuem uma miríade de informação que permite a analistas produzirem *intelligence* "about most events without any more than open sources to spur the process" (Hulnick, 2006: 961). Neste sentido, a adição de *intelligence* nova

proveniente de sensores técnicos ou humanos poderá alterar o processo analítico – raciocínio – mas, raramente o dirige.

O papel desempenhado por analistas é o de avaliar os dados e colocá-los em contexto. Para isso, recebem material de diversas fontes[42]. Hulnik (2006: 961), ao partilhar a sua experiência enquanto analista da *intelligence* militar e da Central Intelligence Agency (CIA), refere que "raw reports from human sources or technical sensors are sometimes fragmentary, biased, contraditory, or just playing wrong*"* e que por norma, para ser possível analisar os dados, o analista compara o novo material com aquele existente em bases de dados e em análises prévias. Para além do mais, efectuar relatórios apoiados nos dados fornecidos por uma só fonte, pode enviesar todo o processo e traduzir-se num resultado errado, o que produz um efeito bastante nocivo para a decisão. James Risen, no livro *State of War* deixa pistas nesse sentido. Segundo aquele autor a *intelligence* que despoletou a invasão do Iraque, em 2003, tinha como base uma única fonte, um suposto cientista iraquiano que havia desertado para os EUA. Não obstante os esforços de Charlie Allen[43] para confirmar os dados daquela fonte, o "Directorate of Operations, (…) was jealous of Allen's incursions into its operational turf and shut down his program and denigrated its results" (Risen, 2006: 106), o que implicou que a análise fosse centrada nos dados facultados por uma só fonte que, pelo resultado final, demonstrou ser pouco credível.

Depois, porque o processo de pesquisa e de análise operam "in parallel rather than sequentially" (Hulnick, 2006: 961). Segundo aquele autor é frequente em vários SIN, como por exemplo nos EUA, os relatórios da pesquisa serem distribuídos para a análise e para os decisores simultaneamente, o que vai criar sérios problemas à análise. Por norma, os decisores tomam essa informação como tendo sido julgada e avaliada e na verdade são relatórios de dados oriundos de fontes humanas ou técnicas o que em última análise, poderá levar a uma contradição entre os relatórios da pesquisa e da análise, criando uma dificuldade acrescida em termos de confiança nos SIN, e com isso o intensificar da barreira da comunicação entre decisores e SIN. De mais a mais, as dificuldades de comunicação são reforçadas em função de algumas barreiras à comunicação, muitas delas psicológicas, restrições provocadas por partilha de *intelligence*, o medo de comprometimento de fontes, desconfiança na qualidade dos relatórios da pesquisa e preocupações de segurança, tornando as etapas de pesquisa e análise, mais que processos paralelos, processos, de alguma forma, independentes. Por certo "the ideal state is one in which (…) collectors act in response to analytic needs and not independently or opportunistically" (Lowenthal, 2006: 62).

Por fim, a disseminação, a etapa que deve alimentar o processo de decisão. Todavia, na realidade essa situação depende do tipo de informação disseminada. De facto, o decisor só faz uso do

[42] Incluindo dos média, relatórios oficiais de outras agências do governo, bem como, relatórios cuja origem é o processo de pesquisa.

[43] Um quadro superior da CIA, na época.

conhecimento, facilitado pelo SIN, se assim entender. Na realidade, de acordo com Hulnik os decisores muitas das vezes têm a noção da modalidade de acção escolhida, necessitando, apenas de *intelligence*, para confirmar a sua escolha. No caso de a *intelligence* infirmar a referida opção os decisores podem prescindir dela. Quando confirma aquilo que presumem conhecer, os decisores podem percepcionar o produto enquanto uma confirmação, irrelevante ou inútil (2006: 967).

Após uma análise do diferencial entre o modelo, que representa o ciclo de produção de informações, e a realidade, Lowenthal (2006), à semelhança de Treverton (2003) ou Clark (2004), detecta a necessidade de alterar o modelo de modo a espelhar a realidade e criar condições para, à semelhança de outro processo, encontrar mecanismos de eficácia. Assim, propõe a inclusão de duas fases, para além da disseminação. O consumo e o *feedback*. A primeira, associada à etapa da disseminação, pretende identificar quais os factores e *trade-offs* entre os objectivos conflituais dos decisores e dos SIN, de forma a ir ao encontro das necessidades e preferências dos decisores e ajustá-las quando há mudança de administração ou governo. A segunda, pretende ultrapassar as barreiras de comunicação entre decisores e SIN, que segundo aquele autor são "at best imperfect throughout the intelligence process" (Lowenthal, 2006: 64). Segundo Lowenthal, os decisores deveriam, idealmente, fornecer um contínuo *feedback* aos seus SIN tendo em consideração o que foi útil ou não, que áreas se deve continuar a dar ênfase ou incrementar o esforço de *intelligence*, quais as áreas que se deve reduzir o enfoque da *intelligence*, entre outros. Todavia, os SIN recebem o *feedback* com menor frequência que desejariam ou não o recebem de forma sistemática. Primeiro, porque são poucos os decisores que possuem tempo para pensar sobre o assunto. Em segundo lugar, poucos decisores pensam que o *feedback* é necessário, mesmo quando a *intelligence* que recebem "is not exactly what they need*…"* (Lowenthal, 2006: 64).

O problema da comunicação assume, então duas dimensões. A primeira entre SIN e decisores na etapa da definição do problema – ausência da orientação do esforço de pesquisa – e após a disseminação – a ausência de *feedback* – que poderá facilitar a introdução de medidas correctivas no processo de geração de conhecimento. A segunda dimensão, interna por natureza, prende-se com o «divórcio» entre a pesquisa e a análise, o qual pode gerar defeitos no conhecimento – o produto do processo – seja em termos de oportunidade, seja relacionado com a relevância – adequação às necessidades do decisor.

2.2. O Produto

É o conhecimento que alimenta o processo de decisão e é através deste que, à semelhança da definição dos requisitos, os SIN se ligam, formalmente, aos decisores. Nesse sentido entendemos o conhecimento como um corpo de informação e conclusões esboçadas dos dados recolhidos e analisados que "…helps policymakers, decision makers, and military leaders carry out their mission of formulating and implementing national security policy" (Goldman, 2006: 83-84).

Tendo como base de partida o conhecimento, este pode-se manifestar, de acordo com Shulsky e

Schmitt (2002: 57-61), em relatórios formais de *intelligence* estratégicas[44] e tácticas[45] que se distinguem pelo seu enfoque no passado, no presente e no futuro. São relatórios de *intelligence* básica, *intelligence* corrente, indicadores e alertas e estimativas.

As primeiras, a *intelligence* básica é a compilação de todos os dados disponíveis de interesse geral para decisores e outros membros do sistema de *intelligence*. É "factual, fundamental, and relatively permanent information about all aspects of a nation (…) which is used as a base for intelligence products in the support of planning, policymaking, and military operations"[46] (Goldman, 2006: 8). É, sobretudo, *intelligence* de carácter estratégico cujo enfoque é colocado em eventos passados e actuais com impacto na política externa de um Estado ou na estratégia de um actor. É, assim, "fundamental, comprehensive, encyclopedic, and general reference-type material relating to political, economic, geographic, and military structure, resources, capabilities, and vulnerabilities of foreign nations" (Goldman, 2006: 8). São, na essência, de natureza descritiva.

A *intelligence* corrente é referida à *intelligence* que é gerada e disseminada numa base diária. É *intelligence* de todos os tipos e formas que fazem referência a eventos de interesse imediato "…characteristically focusing on descriptive snapshots of generally static conditions" (Goldman, 2006: 29). É informação perecível que é disseminada no imediato e que pode, pela premência da decisão, apresentar algumas vulnerabilidades como a falta de uma avaliação completa, interpretação ou integração. É comparável, para Shulsky e Schmitt (2002: 2-4), com as notícias veiculadas pelos órgãos de comunicação social, são como que *flash news*. Mark Lowenthal acrescenta, ainda, que a *intelligence* corrente será conhecimento acerca de assuntos cuja pertinência não se estenderá "…more than a week in the future*"* (2006: 111). Segundo aquele autor, esta tipologia de produto de *intelligence* é o esteio principal dos sistemas de *intelligence*, "…the product most often requested and seen by policy makers*"* (Lowenthal, 2006: 111).

No atinente a indicadores e alertas podemo-nos referir como sendo um termo genérico associado às actividades de *intelligence* necessárias para identificar e relatar conhecimento sensível em termos de oportunidade acerca de eventos que possam ameaçar "a country's allies, its citizens abroad, or the country's military, economic, or political interests" (Goldman, 2006: 67), isto é, o interesse nacional. São o que Shulsky e Schmitt (2002: 58) qualificam como sendo a tarefa mais valorizada no

[44] Entende-se *intelligence* estratégica a *intelligence* que é necessária para a formulação de "…policy and military plans at national and international levels" (Goldman, 2006: 127). As suas componentes incluem, de acordo com o mesmo autor, "…such characteristics as biographic data, economic, sociological, transportation, telecommunications, geography, political, and scientific and technical intelligence" (Goldman, 2006: 127)

[45] Para Goldman, *intelligence* táctica é a *intelligence* necessário ao "…planning and conduct of tactical operations" (2006: 130). Na essência, a *intelligence* táctica e estratégica difere no âmbito, ponto de vista e nível de emprego dos meios do Estado. Com a *intelligence* táctica procura-se, segundo o mesmo autor "…to gather and manage diverse information to facilitate a successful prosecution of the intelligence target. TI is also used for specific decision making or problem solving to deal with an immediate situation or crisis" (Goldman, 2006: 130).

[46] São o aspecto físico, social, económico, politico, biográfico e cultural.

desempenho de um órgão de *intelligence*, o de alertar os decisores de forma atempada o eclodir de uma crise[47], como que de um alarme se tratasse.

Por fim, as estimativas, que derivam da análise, desenvolvimento ou tendências, de uma situação – identificando e interpretando os seus elementos principais – de modo a avaliar as possibilidades e potenciais consequências que daí podem ocorrer. Pretende-se, com as estimativas, efectuar a avaliação das capacidades, vulnerabilidades e intenções de forma a identificar potenciais modalidades de acção (Goldman, 2006: 49) de determinado actor adversário – Estatal ou não-Estatal. Para Shulsky e Schmitt, as estimativas, são uma projecção da situação corrente tendo como base uma análise objectiva de todos os dados disponíveis e no estudo da probabilidade e possibilidade de evolução (2002: 61). Serão a base dos cenários[48] que permitem apoiar o planeamento estratégico e, assim, prevenir a surpresa estratégica.

Contudo, nem todos os tipos de produto merecem a mesma atenção por parte dos decisores, o que produz impacto na comunicação entre decisores e SIN e, consequentemente, na capacidade de antecipação, isto é, na capacidade de evitar a surpresa estratégica, existindo uma diálise que favorece a *intelligence* corrente – centrada no presente – em detrimento das estimativas – centradas no futuro.

De acordo com Lowenthal, é a *intelligence* corrente que "pays the rent for intelligence comunity*"* (2006: 111) uma vez que, segundo aquele autor, a *intelligence* corrente tem predominância sobre os outros tipos de *intelligence*. Porém, o grau de predominância varia de acordo com o tempo, em virtude da situação que se vive. Assim, durante uma situação de crise ou guerra a *intelligence* corrente obtém um incremento já que a maioria das decisões, neste período são tácticas, por natureza "…even among senior policy makers" (Lowenthal, 2006: 111). Como por exemplo verificável nas questões relacionadas com a necessidade de *intelligence* acerca de ADM iraquianas ou relativas à Guerra Global Contra o Terrorismo (GWOT).

Outra razão para este fenómeno está firmada na interacção com os políticos e na percepção que estes têm sobre a utilidade do conhecimento. Neste sentido, Lowenthal observa que "…few policy makers are likely to read papers with longer orizons" (2006: 111), não por falta de interesse mas, por falta de tempo e incapacidade de se abstrair dos assuntos que os pressionam, no momento. Assim, a escolha dos decisores recai, naturalmente, sobre a *intelligence* corrente que tende a possuir um menor horizonte temporal em virtude da sua natureza e dos objectivos que cobrem.

Fruto da sua dimensão temporal, os produtos de *intelligence* corrente limitam a possibilidade dos

[47] Uma crise pode ser entendida como a "convergence of rapidly unfolding events in an outcome that is detrimental to national security" (Goldman, 2006: 26) cujo resultado é, em certa medida indeterminado. Pode ser entendida, também, como o "critical timing and decisionmaking under extreme personal and organizational stress" (Goldman, 2006: 26).

[48] Os cenários de *intelligence* são descrições do modelo de um futuro alvo. O planeamento apoiado em cenários é, normalmente, usado para explorar possíveis condições futuras tendo como base um conjunto de pressupostos. "Each scenario represents a distinct, plausible Picture of a segment of the future*"* (Clark, 2004: 173)

analistas aprofundarem mais a questão em apreço ou de acrescentarem um contexto mais detalhado. Para além do mais, as competências exigidas a um analista para produzir *intelligence*, corrente ou estimativa, são diferentes. Sendo o número de analistas de um SIN limitado, há a necessidade de alocar os meios humanos de acordo com o empenhamento que é solicitado. Neste sentido, mantém-se a predominância da *intelligence* corrente sobre a estimativa, quer em termos de recursos, bem como na forma como os decisores percebem o SIN.

Em suma, ao colocar o foco do esforço de um SIN na *intelligence* corrente está a afectar-se a capacidade de antecipação, já que esta tipologia de *intelligence* se centra no presente ou num futuro próximo. Porém, Mark Lowenthal nota que a *intelligence* pode ser corrente e estratégica (2006: 112). Corrente, em virtude do foco temporal e estratégica ao procurar providenciar um contexto mais alargado ou mais inter-relação com outras questões, por exemplo. Isto é, procurar acrescentar valor e, concorrentemente, incrementar a qualidade do produto – reforçando a capacidade de antecipação – o que implica, necessariamente, uma maior relação de confiança entre SIN e decisores e, consequentemente, uma maior capacidade de comunicação.

Uma forma de poder identificar a qualidade do *output* do processo de análise da *intelligence* será recorrendo ao que Sherman Kent se referia como sendo os três desejos de um analista: saber tudo, ser credível e influenciar a política (Lowenthal, 2006: 139). Com o primeiro, Kent, procurava expressar que um analista de *intelligence* deverá saber tanto quanto possível sobre determinado assunto antes que seja solicitado a escrever sobre ele, isto é, garantir a antecipação de determinados assuntos. Para isso, deverá possuir competências que lhe permitam desenvolver capacidades para "…reed between the lines, to make educated guesses or intuitive choices when the intelligence is insuficient…" (Lowenthal, 2006: 139).

O segundo desejo de Kent, ser credível, centra-se no cerne das relações entre decisores e SIN. Os decisores "pay no price for ignoring intelligence, barring highly infrequent strategic disasters" (Lowenthal, 2006: 139), como por exemplo a recusa de Estaline aceitar uma invasão alemã, que se veio a materializar na operação Barbarrossa, em 1941, ou na rejeição pelo *British Foreign and Commonwealth Office* da percepção de uma invasão argentina às Malvinas (Clark, 2004: 1-2). Os oficiais de *intelligence*[49] veêm-se como alguém honesto e com objectividade, que pretende, apenas, acrescentar valor ao processo que providencia a análise. A sua recompensa, no fim do processo, é serem ouvidos, isto é, que haja comunicação (Lowenthal, 2006: 140).

Finalmente, e decorrente do desejo anterior, Kent observa que os oficiais de *intelligence* pretendem ter um impacto positivo na decisão. Porém, esse desejo não se fixa apenas nos *outcomes* do processo, esta pretensão indica que há o desejo de os oficiais de *intelligence* se manterem informados acerca das

[49] Um oficial de *intelligence* é "… a professional employed by an intelligence service" (Lerner e Lerner, 2004: 133)

actividades dos decisores, de modo a que o seu desempenho tenha sentido no contexto da decisão (Lowenthal, 2006: 140). Isto é, o desejo de Kent centra-se na comunicação entre decisores e SIN. Que será tão mais facilitado quanto melhor for o conhecimento.

É do conhecimento geral que a *intelligence* gerado por SIN, para ser considerado útil para a decisão, terá de possuir, pelo menos, duas características: ser oportuno e relevante. A oportunidade implica que é mais importante fazer chegar a *intelligence* aos decisores, de forma a ser utilizada no processo de decisão, que esperar pela última peça de informação da pesquisa para elaborar um documento «limpo», no formato desejado, mas, que seja extemporâneo para a decisão.

A relevância, por seu turno, procura fazer reflectir a importância que determinada *intelligence* detém num determinado contexto de decisão. Por exemplo se o foco da decisão é o Médio-Oriente, provavelmente *intelligence* relativa a outra área do globo pode ser considerada irrelevante para a decisão.

Ao debater a questão da qualidade do produto, e como é que ela pode ter impacto na confiança depositada por decisores num SIN – cujo impacto é decisivo em termos de comunicação[50] – Lowenthal tem como ponto de partida os desejos identificados por Kent e observa que para que o conhecimento possa ser considerado de qualidade deverá possuir quatro características: a oportunidade; ser talhado às necessidades; ser «digerível»; e, separar o conhecido do desconhecido.

A primeira, a oportunidade, debatida anteriormente, prende-se, essencialmente, com o *timing* da recepção da *intelligence* para ser incorporada no processo de decisão, e vai ao encontro do primeiro desiderato de Kent. Pois, se o analista tiver conhecimento das necessidades dos decisores, em antecipação, provavelmente a *intelligence* chega aos utilizadores sem se arriscar a possibilidade da inoportunidade. Importa, então, a antecipação, o «saber tudo» que Kent deseja (Lowenthal, 2006: 140).

A segunda, ser adequado às necessidades, foca-se nas necessidades específicas de *intelligence*, expressas pelo decisor. Deverá ser conduzido de forma a não perder a objectividade ou deixar que seja politizada. O conhecimento adequado, às necessidades específicas dos decisores, é aquele que obtém um maior grau de prioritização, por parte daqueles que o solicitam (Lowenthal, 2006: 140).

Em terceiro lugar surge a capacidade de ser «digerível». Com esta característica Lowenthal pretende alertar para que a *intelligence* terá de ser transmitida numa forma e dimensão tal que permita aos decisores uma compreensão fácil do conhecimento. Os requisitos de informação tendem a facilitar produtos de *intelligence* de menores dimensões, mas a sua principal função é a de sublinhar que a mensagem deve ser apresentada de forma clara para que seja mais facilmente percebida. O que não significa que a mensagem não possa ser complexa ou incompleta. Todavia, independentemente da

[50] Se os decisores não possuírem confiança num SIN, provavelmente a comunicação entre ambos passa a ser mais dificultada. Pelo que por parte do SIN importa garantir um produto de qualidade de forma a estabelecer e manter essa relação de confiança e, com isso, facilitar a comunicação entre ambos.

complexidade da mensagem, o decisor deverá ter condições para percebê-la despendendo o mínimo de energia (Lowenthal, 2006: 140). Deve ser transmitido de forma clara.

O separar o conhecido do desconhecido é a quarta característica que o conhecimento deverá obedecer em termos de qualidade. Deve ser transmitido ao utilizador, de forma inequívoca, o que se conhece, o que não se conhece e o que foi elaborado na análise, bem como o grau de confiança no material. O grau de confiança assume especial importância dado que o decisor deverá ter algum sentido de relativização da sustentação da *intelligence*. Devido à sua natureza toda a *intelligence* envolve risco[51] em virtude da natureza da informação com que lida. Nesse sentido, o grau de confiança da *intelligence* é uma forma dos SIN partilharem esse risco com os seus utilizadores (Lowenthal, 2006: 140). Deverá, acima de tudo, garantir a credibilidade do produto junto do utilizador, isto é, deverá ser inequívoco.

Para aquele autor a objectividade não deve ser considerada uma característica, porque deve ser considerada, *a priori*, como um dado assente. Acrescenta ainda que se a *intelligence* não for objectiva, então todas os outros atributos perdem relevância. A exactidão, outro factor por norma associado à qualidade do conhecimento, também não deve ser considerada como característica. Para Lowenthal, a exactidão, é difícil de identificar porque, ainda que ninguém pretenda falhar, toda a gente reconhece a impossibilidade de infalibilidade. Nesse sentido, torna-se difícil de perceber qual a percentagem de infalibilidade aceitável. Este factor, tornou-se particularmente importante após o 11 de Setembro de 2001 e no inicio da guerra do Iraque, onde o sistema político se tornou menos tolerante à imperfeição inerente à análise de *intelligence* e ao conhecimento daí decorrente. Assim, "even though all observers understand that perfection is not possible, each and every mistake seemed to incur a large political cost for the intelligence agencies*"* (Lowenthal, 2006: 141).

Contudo, ainda que o processo seja falível, é impossível produzir conhecimento de qualidade. Lowenthal (2006: 142) refere que para se atingir um produto de qualidade aceitável deverá haver um esforço adicional, o de distinguir do padrão do fluxo da *intelligence* produzida diariamente, a quantidade de *intelligence* inserida e aquela que fica «de fora» e a razão pela qual não é adequada[52].

Em suma, parece-nos que acerca do debate sobre da qualidade do conhecimento não restam dúvidas relativamente à característica oportunidade. Quanto à característica relevância, para Lowenthal, esta englobará os elementos: ser adequado às necessidades; ser «digerível»; e, separar o conhecido do desconhecido. Nesse sentido, será, em nosso entender oportuno associar a relevância em termos de: adequabilidade – às necessidades dos decisores; clareza – em termos de transmissão e da forma como se transmite a ideia; e, distinção – não deixando dúvidas acerca do que se conhece e do que não se conhece, bem como da avaliação da verosimilhança da *intelligence*.

[51] Risco é, para Jan Goldman, a "probability that a particular threat will exploit a particular vulnerability of the nation's security that will result in damage to life, health, property, or the environment" (2006: 121).
[52] A oportunidade, a qualidade do documento ou o seu efeito no processo de decisão, entre outros.

> *"O Senhor falou a Moisés: «Manda homens para explorar a terra de Canaã, que Eu hei-de dar aos filhos de Israel» (...) Moisés enviou-os a explorar a terra de Canaã e disse-lhes: «Subi o Négueb, subi a montanha. Vede que terra é essa e que povo habita nela, se é forte ou fraco, pouco ou muito numeroso (...) Que cidades habita, abertas ou fortificadas?» "*
>
> Nm 13, 1-23[53]

CAPÍTULO III – AS FUNÇÕES

Com a desintegração do «Bloco de Leste» e o recrudescimento de determinados desafios[54] surgem novas prioridades no quadro da segurança dos Estados, patentes na alteração significativa da natureza dos requisitos de *intelligence*. Assim, contrariamente aos conflitos entre Estados, maioritariamente militares, onde havia um inimigo declarado, surgem inimigos sem rosto que operam, em grupo ou isoladamente, "spacialy obscure, organizationally fluid, and often opaque*"* (Ellis, 2010: 2). Desde o fim da guerra fria a instabilidade provocada por estes fenómenos veio expandir as fronteiras das áreas de interesse do Estado de forma avassaladora, numa lógica que sugere que a complexidade, relativamente às actividades desenvolvidas por SIN, tenha aumentado em igual proporção.

O paradigma da *intelligence*, resultante da guerra fria, era centrado essencialmente nos Estados, que por definição, para além de território tem também população e órgãos de decisão[55]. Nesse sentido, podemos inferir que, em primeiro lugar, os Estado apresentam padrões verificáveis ao longo do tempo (a história), são geográficos e burocráticos o que, em certa medida, oferece alguma previsibilidade nas suas acções. Em segundo lugar, entre Estados opositores, a interacção era relativa. Procurava-se influenciar o oponente com determinadas políticas, ou seja, esperava-se uma reacção, a qual nem sempre seria visível[56]. Em terceiro lugar, os decisores que necessitavam da *intelligence* estavam identificados como sendo os decisores políticos e militares, ainda que a informação disponível fosse parca e assentasse, fundamentalmente, em fontes secretas. O principal «alvo» das actividades da *intelligence* ocidental era a URSS e os seus Estados satélites, cujo regime fechado limitava a informação em fontes abertas. Em quarto lugar, o produto da *intelligence* assentava no que Gregory

[53] Livro dos Números in Bíblia Sagrada (1998).

[54] Como o terrorismo internacional, a proliferação de ADM, o narcotráfico, as ameaças económicas, ameaças à saúde e ambiente, entre outros.

[55] Para o Professor Marcello Caetano o Estado é "um povo fixado num território de que é senhor, no interior de cujas fronteiras institui, por autoridade própria, órgãos que elaboram as leis necessárias à vida colectiva e impõe a sua execução*"*. (Caetano, 1967: 117)

[56] Veja-se por exemplo a competição nuclear entre EUA e URSS, na qual o desafio era o de perceber qual a provável modalidade de acção dos contendores e não a calibração da influência de outras nações nessa modalidade.

Treverton designa de *puzzles*[57], em contraponto aos mistérios[58] – uma vez que se procurava aceder a informação acerca das capacidades[59]. Esse produto enformava as «peças adicionais» para preencher o «mosaico da informação». Em quinto lugar, a estratégia dominante durante a guerra fria assentava na dissuasão, que para Treverton (2009: 37) era ancorada na ideia de que, para além das diferenças ideológicas, a URSS e os EUA eram ambos modernos, racionais e não auto-destrutivos. As intenções soviéticas eram percebidas como hostis, mas racionais. A partir do momento que Moscovo passou a deter ADM a forma de garantir de que estas não eram usadas foi através da estratégia de dissuasão[60]. Para aquele autor a *intelligence* teve um papel importante, ainda que não tenha sido vital. As necessidades de *intelligence* centravam-se nas capacidades[61] e nas intenções e percepções[62].

Após o colapso do bloco soviético os Estados ainda se colocam como oponentes aos seus semelhantes[63], no entanto com o segundo milénio surgiram outros «alvos». São os actores transnacionais que variam desde grupos terroristas, a negócios internacionais.

Se os Estados podem ser caracterizados, de acordo com Treverton (2009: 16) em Estados fechados[64], Estados mistos[65] e Estados abertos[66] os segundos são aqueles que vêm pressionar, com mais veemência, as alterações ao paradigma da *intelligence*. Assim, em primeiro lugar, estes «alvos» não são geográficos, muitas vezes[67] não têm uma hierarquia definida e não são, por norma,

[57] *Puzzles* são questões a que se pode dar resposta com algum grau de certeza tendo como recurso a informação, em princípio, disponível. Isto é, consegue encontrar-se uma relação de causa-efeito. O desafio está, de acordo com Treverton, em categorizar correctamente o problema, encontrar a informação necessária e aplicar as fórmulas aceites (2009: 17).

[58] Para Treverton (2009: 146), mistérios são questões que nenhuma evidência pode responder de forma definitiva. São tipicamente acerca de pessoas, e não de bens materiais. São contingenciais. Por exemplo a taxa de inflação da Zona Euro para 2012, é um exemplo do que é um mistério, para aquele autor.

[59] Capacidade é a "possibilidade de um país ou coligação de países executarem determinado tipo de acções*"* (Ribeiro, 2008: 32). A possibilidade que o autor nos refere traduz-se em meios humanos, financeiros e materiais. São estes meios que garantirão a determinado Estado ou coligação as condições que possibilitam atingir objectivos e salvaguardar interesses.

[60] A propósito das decisões racionais veja-se, por exemplo, o resultado da crise dos mísseis de Cuba, em 1962.

[61] Como por exemplo a quantidade de ogivas que Moscovo possuía, numa perspectiva de perceber de que forma as capacidades nucleares eram uma ameaça para os EUA e aliados da NATO.

[62] Como por exemplo qual era o risco que a liderança política soviética estava disposta a correr em caso de guerra nuclear.

[63] Mantendo-se como «alvos» das estruturas de *intelligence*.

[64] O caso da Coreia do Norte, por exemplo, cujas capacidades básicas se matem secretas, sendo que a *intelligence* se foca em puzzles, e as fontes da pesquisa são secretas, uma vez que por definição, num regime fechado, a informação é em pouca monta.

[65] Como o caso da China e Irão, por exemplo, cujos puzzles se mantem, relativamente às capacidades, mas os mistérios ganham importância – as fontes secretas são importantes mas as fontes abertas ganham uma dimensão maior que os anteriores.

[66] O caso dos Estados Ocidentais, por exemplo, cujas capacidades são transparentes e os mistérios ganham uma dimensão avassaladora – as fontes secretas têm menos valor que nos Estados anteriores sendo o problema maior a quantidade grande de informação.

[67] Principalmente os actores relacionados com actividades criminosas (grupos terroristas, grupos de tráfico de droga, entre outros), ainda que grupos económicos transnacionais, por exemplo, não tenham a mesma estrutura dos Estados ou hierarquia. Se o padrão de comparação é o Estado, então, parece-nos adequado referir que estes actores também não são burocráticos e a hierárquicos.

burocráticos. São desterritorializados e não se consegue identificar um padrão de actuação, o que origina a falta ou ausência de contexto. Em segundo lugar, há uma interacção grande entre o Estado e esta tiologia de «alvos»[68]. Em terceiro lugar, os «alvos» não-estatais estão menos limitados. A falta de constrangimentos garante a necessária liberdade de acção para desenvolver determinadas actividades[69]. Em quarto lugar, desde que o mundo despertou para os fenómenos colocados por «alvos» transnacionais e os consumidores de *intelligence* deixaram de ser, apenas, os decisores políticos e militares[70].

Em quinto lugar, em virtude da natureza transnacional dos «alvos» os SIN encontram-se confrontados com uma miríade de informação que contrasta com a nitidez da informação, ainda que em muito menor quantidade, própria dos tempos da guerra fria. Pelo que separar a informação de «ruído» é, na actualidade, uma tarefa de grande monta.

Em sexto lugar, os «alvos» transnacionais envolvem *puzzles* e mistérios, mas envolvem, também, aquilo que Treverton (2009: 33) designa de complexidades[71]. "Large numbers of relatively small actors respond to a shifting set of situational actors. Moreover, because interactions reflect unique circumstances, they do not necessarily repeat in any established pattern and are thus not amenable to predictive analysis in the same way as mysteries" (2009: 146). Em sexto lugar, a estratégia deixou de estar associada à dissuasão, está associada à prevenção. Nesse sentido, as necessidades de *intelligence* deixam de ser importantes, passam a ser vitais. Tal como na dissuasão a lógica da prevenção é evitar o confronto, contudo, tal só é possível se os «alvos» forem sujeitos à disrupção ou se evitar que acedam às vulnerabilidades do objectivo eleito. Para tal, é necessário os SIN ternham uma compreensão bastante apurada das ameaças em tempo.

Fruto dos desafios que o ambiente coloca, estruturas de *intelligence* têm de desenvolver actividades de modo a garantir que o conhecimento é gerado, tendo em vista o necessário valor-acrescentado para a tomada de decisão e é assegurada a necessária segurança, seja nos processos, fontes, necessidades ou outros. Nesse sentido, seguindo a abordagem holística a que nos propusemos, importa tratar aqueles que Shulsky e Schmitt designam de elementos da *intelligence*. São as funções[72]: pesquisa, análise,

[68] Os grupos terroristas, por exemplo, alteram as suas capacidades em função das vulnerabilidades do seu objectivo, o que, em termos de intelligence, torna a dimensão externa e interna transversais, ao invés da estanquicidade, própria do paradigma bipolar.

[69] Por exemplo, actividades financeiras – muitas empresas transnacionais possuem orçamentos que ultrapassam os governos, tornando-se interlocutores de peso nos mercados financeiros internacionais – ou atentados que produzem vítimas em massa.

[70] A título de exemplo Treverton refere que "an aiport security officer or a public health doctor may have a more urgent «need to know» about a threat than the president of the United States because he or she may be in a more immediate position to thwart it" (2009: 29).

[71] Complexidades são designadas por Treverton (2009: 146) como mistérios-mais. Envolvem uma série de causas e efeitos que podem interagir numa variedade grande de maneiras, de forma contingencial.

[72] Entendemos função na sua acepção fundamental que, de acordo com Morujão (1985: 768), corresponde a operação.

counterintelligence e acção coberta. Contudo, Boraz e Bruneau (2006: 30) alertam para o facto de que, ainda que as quatro funções definam a ancoragem no qual o problema das informações deve ser entendido, nem todos os Estados tem a necessidade, o querer ou a capacidade de possuir vastas capacidades em todas as funções, no entanto, quase todos os Estados conduzem, pelo menos, algumas actividades de informações detendo, para o efeito, alguma organização de informações.

As duas primeiras são entendidas numa lógica de geração de conhecimento. As restantes são percebidas numa perspectiva de protecção e disrupção das actividades, capacidades e intenções, de forma a negar o conhecimento necessário para alimentar o processo de decisão do adversário.

3.1. A pesquisa

As capacidades de pesquisa da maioria dos Estados ocidentais tem como base toda uma miríade de meios[73] desenvolvidos durante o período da guerra fria, de forma a dar resposta às dificuldades de penetração na URSS[74] cujos principais alvos eram de cariz militar. No entanto, apesar das alterações significativas no objecto da pesquisa de *intelligence*, esta função mantém-se como uma actividade fundamental para a geração de conhecimento. É, por norma, entendida como a pedra basilar da *intelligence*. É através desta que se acede aos dados acerca das actividades, capacidades e intenções do adversário que permitem acrescentar valor à informação.

Nesse sentido, a função pesquisa[75] utiliza vários métodos[76] ou disciplinas, as quais podem ser sistematizadas, de acordo com Shulsky e Schmitt (2002: 11), em pesquisa com recurso a: meios técnicos (TECHINT), HUMINT e à OSINT.

Cada um destes métodos de pesquisa, de acordo com Lowenthal (2006: 79), apresenta vantagens e inconvenientes, no entanto quando se faz a avaliação dos mesmos será importante recordar que o objectivo será envolver o máximo de métodos possíveis, principalmente em situações de maior premência para o decisor. Esta postura permitirá, porventura, a sinergia que compensa as insuficiências e desvantagens que cada uma apresenta *per se.*

A primeira, a TECHINT, possui algumas vantagens comuns, para além daquelas que cada um dos seus elementos (IMINT, SIGINT e MASINT) apresenta, não deixando, no entanto, de serem complementares. Primeiro, permite a operação remota dos sensores que utiliza, não colocando, por isso, em perigo a vida de humanos e tornando, ainda, as intenções dos decisores menos «visíveis» a

[73] Principalmente técnicos.

[74] Uma sociedade fechada com uma grande vastidão de massa terrestre, más condições meteorológicas e uma longa tradição de secretismo e decepção

[75] A pesquisa, segundo Lowenthal (2006: 68), cobre três tipos diferentes de actividades: a *Intelligence* (termo genérico para a pesquisa); a vigilância (a observação sistemática de uma alvo – área ou grupo – por um período de tempo, geralmente alargado); reconhecimento (missões para adquirir informação acerca de um alvo, por vezes designa uma empresa única no tempo).

[76] Que se pode entender como um "conjunto de procedimentos e de regras para se chegar ao resultado desejado*"* (Russ, 2000: 198).

possíveis adversários. Depois, são métodos, principalmente a IMINT e SIGINT, que podem com mais facilidade adquirir alvos com grande volume, como as actividades de forças militares (Lowenthal, 2006: 79-94).

Individualmente, a IMINT oferece como principais vantagens o facto de ser gráfica e cativante e de fácil interpretação (Lowenthal, 2006: 83-84).

A SIGINT tem como principal vantagem o acesso a planos e intenções do adversário, através da exploração e intercepção das comunicações. Permite, em última análise, ler "the other side's mind, a goal that cannot be achieved by imagery" (Lowenthal, 2006: 90), à distância. Para além de aceder a uma grande quantidade de dados, obtidos pela exploração das comunicações. No mundo globalizado os meios de comunicação incrementaram enormemente[77] pelo que é possível utilizar sistemas de intercepção da tipologia *echalon*[78], em que o acesso à informação, com provável valor de intercepção, se faz com recurso a pesquisas por palavras-chave (Lowenthal, 2006: 91).

A MASINT centra-se essencialmente no que concerne a actividades industriais e desenvolvimento de armamento. Identifica tipos de gases ou resíduos fabris – o que poderá ser de capital importância na detecção de ADM, concretamente o armamento químico – para além de identificar características específicas[79] de sistemas de armas (Lowenthal, 2006: 93). É neste contexto que apresenta as suas vantagens, principalmente numa época em que a proliferação de ADM, o controlo de armamento, os problemas ambientais e o narcotráfico, são algumas das principais preocupações em termos de segurança.

Contudo, a TECHINT apresenta algumas desvantagens. O facto de necessitar de sensores tecnologicamente desenvolvidos, principalmente aqueles que dependem de satélites, torna esta actividade muito dispendiosa. Para além do mais, a dependência de satélites impõe alguma falta de flexibilidade para o emprego dos sensores que deles dependem para operar, já que aquelas plataformas são programadas para operar em determinadas órbitas fixas[80].

Individualmente os seus elementos apresentam algumas desvantagens, sendo os aspectos operativos aqueles que entram em maior monta.

A IMINT é um método estático, isto é, é literalmente um fotograma de um determinado momento *tells you what has happened*. Em segundo lugar, está dependente das condições meteorológicas. Em terceiro lugar, as ameaças colocadas por pequenos grupos, pelas suas características[81], deixam uma

[77] Telefones, telefones móveis, faxes, e-mails ou tecnologia VoIP (*Voice-over-Internet-Protocol* – permite a utilização de telefones via internet).

[78] Sistema de intercepção de comunicações global operado "by means of cooperation proportionate to their capabilities among the USA, the UK, Canada, Australia and New Zealand under the UK-USA Agreement…" (Schmid, 2001).

[79] Composição e material

[80] Sendo um bom exemplo o caso das Malvinas descrito no capítulo 3.

[81] As células são mais pequenas, menos elaboradas e possuem menos visibilidade que os alvos politico-militares tradicionais.

«pegada» muito menor que qualquer actividade militar, pelo que só é possível empenhar a IMINT tendo como «alvo» situações em que seja visível a actividade da ameaça[82] (Lowenthal, 2006: 91).

A SIGINT, para além dos meios necessários à intercepção, carece de meios para a desencriptação, seja do sinal seja do conteúdo da comunicação, uma vez que é expectável que a comunicação por meios electrónicos se efectue num ambiente seguro. Em segundo lugar, está dependente da manifestação de comunicações, já que se existir silêncio[83], torna-se totalmente ineficaz.

O segundo método de pesquisa, a HUMINT, possui como principal vantagem, o facto de garantir o acesso mais facilitado às intenções e planos de adversários, o que permite a identificação de oportunidades *"*to influence that government by feeding it false or deceptive information*"* (Lowenthal, 2006: 97). Além do que, se comparada com a TECHINT, é menos onerosa[84], o que alimenta a convicção que na guerra contra o terrorismo a HUMINT é o método de pesquisa privilegiado (Lowenthal, 2006: 96-97). Para além do mais, garante flexibilidade a outros métodos de pesquisa. Pode providenciar o alerta de que algo poderá ocorrer em determinada região, facilitar a interpretação dos dados colhidos por outro método ou pelo acesso a determinados «alvos» pode servir de sensor para a colocação de sensores de SIGINT, junto a alvos humanos (Lowenthal, 2006: 97).

Em contrapartida, este método apresenta algumas desvantagens operativas. Porque requer a proximidade ao «alvo» é confrontado com capacidades de *counterintelligence* do adversário, o que induz a um risco mais elevado em termos de vida humana e de consequências políticas, decorrentes de ganhos de informação falsa ou enganadora[85], menos passível de ocorrer quando da utilização da TECHINT. É, igualmente, um método pouco flexível[86] e moroso[87].

---

[82] Como por exemplo as infraestruturas de treino.

[83] A comunicação pode ser efectuada recorrendo às *dead letter box* – método usado para a passagem de mensagens ou outros recorrendo a um local secreto, não necessitando por isso o recurso a meios electrónicos ou *face-to-face*

[84] Ainda que envolva custos para treino, equipamento especial, recrutamento e criação de histórias de cobertura (Lowenthal, 2006: 97).

[85] O controlo de qualidade da informação é uma das principais dificuldades da HUMINT. Dependendo das suas motivações as fontes podem «fabricar» informação ou «embelezar» informação disponível através de fontes abertas ou podem trabalhar secretamente para o adversário. No que concerne aos grupos terroristas, como a penetração naquelas organizações depende das lealdades (manifestadas por laços familiares, acções, etc.) este desiderato é bastante difícil pelo que se recorre, normalmente, ao recrutamento de um membro daquele grupo.

[86] A falta de flexibilidade prende-se essencialmente com o facto de as fontes serem recrutadas tendo em conta o seu acesso à informação desejada, pelo que sempre que os requerimentos de informação alterem poderá ter de ser efectuado novo processo de recrutamento.

[87] A morosidade dos resultados é a consequência de um processo de treino de agentes (que de acordo com Lowenthal (2006: 95) o processo de treino de um agente pode levar até sete anos) e de recrutamento e validação de fontes algo demorado que decorre em cinco fases: (*i*) *Targeting* - Identificação de indivíduos com acesso à informação desejada; (*ii*) Acesso - obtenção da sua confiança procurando identificar vulnerabilidades e susceptibilidade do recrutado; (*iii*) Recrutamento - sugerir uma relação pessoal (com base em dinheiro, desagrado com o seu governo, chantagem, e outros); (*iv*) Gestão da fonte - fase em que o agente se reúne com as suas fontes, de forma regular para receber a informação desejada; (*v*) Termo - terminar a relação.

Contudo nem todas as fontes carecem de um processo de recrutamento tão moroso. Para além das fontes recrutadas pelas agências dos SIN, há que considerar outras fontes. São os *walk-ins* e as fontes diplomáticas – embaixadores, adidos, etc. Os primeiros são elementos que se voluntariam para auxiliar uma agência de *intelligence* de um Estado estrangeiro[88] que "sometimes literally by walk into an embassy*"* (Shulsky e Schmitt, 2002: 16). Como estas fontes não são sujeitas ao processo de recrutamento descrito tornam-se inerentemente suspeitos, uma vez que o suposto «voluntarismo» pode decorrer de uma tentativa, do oponente, de passar informação falsa ou enganatória, aceder a métodos operativos ou outros, em suma infiltrar um agente no SIN em questão. As segundas, diplomáticas, são, para autores como Lowenthal e Shulsky e Schmitt, um «composto» de OSINT e HUMINT, já que os ganhos de informação são obtidos num ambiente aberto recorrendo a fontes humanas[89]. Os diplomatas podem providenciar informação acerca da situação de política interna, os adidos militares[90], podem facilitar informação relativamente ao poder militar. A informação obtida pelos canais diplomáticos tende a ser considerada como tendo menos credibilidade em função do ambiente aberto em que opera. Assim, além das percepções pessoais há que ter a noção que qualquer decisor político ou militar sabe que, ao falar com um diplomata, aquela conversa será reportada para a capital do diplomata em questão (Lowenthal, 2006: 95).

Por fim, a OSINT. É um método de pesquisa que não lida, directamente, com a descoberta de segredos. No entanto, segundo Lowenthal (2006: 101), durante o período da guerra fria foi responsável por cerca de vinte por cento da *intelligence* acerca da URSS. Consiste na obtenção de informação com recurso a todas as fontes disponíveis[91] e cujo acesso é permitido sem qualquer medida especial de restrição (Shulsky e Schmitt, 2002: 37-39). Um dos cunhos do mundo pós-guerra fria é o aumento significativo de fontes abertas, o que deixa antever que o número de sociedades fechadas e áreas negadas decresceu substancialmente, basta, tão-somente, recordar a quantidade de Estados do ex-Pacto de Varsóvia que se tornaram membros da OTAN) ou são seus *Partners for Peace* (PfP). A maior vantagem da OSINT é a acessibilidade, isto é, está facilmente disponível, ainda que requeira pesquisa. Necessita de menor processamento que os métodos técnicos e humano, não deixando de ser necessário o processamento, de todo. Outra vantagem é a capacidade de colocar a informação secreta num contexto mais vasto, acrescentando valor a essa informação. Para além do mais, para Lowenthal (2006: 101), torna-se de extrema importância como ponto de partida para a exploração de outros

[88] Como é o caso apresentado na obra de Christopher Andrew e Vasili Mitrokhe (2000), o Arquivo de Mitrokhe.
[89] Sem que para isso haja qualquer processo ou procedimento de recrutamento.
[90] Que têm acesso a exercícios militares e cerimónias – onde é exposto o equipamento – bases aéreas, bases navais ou outras infraestruturas civis ou militares de interesse.
[91] Os *media* – Jornais, revistas, rádio, televisão, e informação digital variada; dados públicos - Relatórios de governos, dados oficiais como orçamentos e demografia, audições, debates legislativos, conferências de imprensa e discursos; fontes profissionais e académicas - Conferências, simpósios, associações profissionais, ensaios académicos e especialistas.

métodos[92].

Lowenthal (2006: 103) alerta que, contrariamente aos outros métodos, a OSINT não possui sensores, uma vez que se espera que os analistas ajam como tal. Para além do mais, ao associar o grande volume de informação inerente à OSINT, facilmente se percebe da dificuldade que representa a tarefa de separar os dados relevantes de outros, ainda que recorrendo a meios digitais e *software* especializado. De mais a mais, as OSINT não são gratuitas[93].

Ao debater a problemática das vantagens e desvantagens, Lowenthal (2006: 104), refere que, pela sua natureza, os diferentes métodos possuem vantagens, adequadas a determinados tipos de requisitos, mas incorporam alguns inconvenientes. Pelo que, ao projectar um conjunto alargado de métodos de pesquisa, numa determinada situação, pode-se acentuar que é possível explorar as vantagens de cada método e compensar as desvantagens de outros, pelas sinergias que criam. Para além do mais, ao ser aplicado mais que um método de pesquisa, aumenta-se a probabilidade de ir ao encontro dos requisitos estabelecidos, em virtude das sinergias que podem criar.

Num SIN, por norma, cada método de pesquisa[94] é tutelada por uma agência. Pelo que, a comunidade de *intelligence* coincide com os elementos que compõem o SIN, isto é, as agências que têm competências de pesquisa de *intelligence* incorporam os referidos SIN. Nesse sentido, em virtude da missão de cada agência, o foco não é igual o que permite a pesquisa de *intelligence* sob pontos de vista diferentes, o que vem incrementar a cooperação e a consequente integração garantindo, não só a quantidade de dados como, a, provável, qualidade da informação gerada na análise[95]. Contudo, porque a tutela da pesquisa de *intelligence* está dividida por entidades diferentes pode trazer constrangimentos no que concerne à partilha de informação e à cooperação entre agências, limitando a integração das mesmas, tornando as agências, por vezes competidoras[96].

3.2. A análise

A análise, comporta actividades – como por exemplo o processamento e disseminação – que permitem o tratamento dos dados da pesquisa de modo a gerar conhecimento que, de acordo com Romana (2008: 98), se for fundamental para o problema irá incorporar o processo de decisão e, assim, garantir a diminuição da incerteza relativamente ao meio. É, por isso, uma tarefa que transcende o

[92] A IMINT pode recorrer a imagens comerciais, pode-se fazer SIGINT na internet (recorrendo a análise de tráfego ou alterações em sítios, a MASINT, por ser relacionada com os aspectos geofísicos também pode recorrer a fontes abertas e a HUMINT através do recurso a especialistas para ampliar o conhecimento.

[93] Ainda que a internet seja gratuita, na sua maioria a fiabilidade dos dados disponíveis não representam mais que três a cinco por cento da pesquisa de OSINT, para além do mais, a aquisição de *media* impressa, bem como os sistemas informáticos que apoiam a gestão da informação são onerosos e a sua necessidade é constante.

[94] Como por exemplo nos EUA e na Grã-Bretanha (Lowenthal, 2006)

[95] Como atesta o relatório do congresso que investigou os atentados de 11 de Setembro.

[96] Para Thomas Hunter (2007: 2), a falta de cooperação entre as agências de *intelligence* é motivada por questões relacionadas com a responsabilidade territorial, o de ganho de prestígio e a disputa pela atribuição de verbas do orçamento do Estado.

estar "sitting down with the collected material, sifting and sorting it, and coming up with a briliant piece of propose that makes sense of it all*"* (Lowenthal, 2006: 110).

A alteração, significativa, dos «alvos» descrita anteriormente vem dar espaço para que Treverton sublinhe que "one critical part of the agenda for reshaping intelligence is analysis, and the need is dramatic*"* (2009: 134). Aquele autor salienta que esta necessidade de reestruturação está associada ao facto dos actuais «alvos» serem «moldáveis» e adaptativos, criando uma indefinição nas distinções entre crime, terrorismo, proliferação de ADM e guerra.

Uma das formas de perceber o problema será partir do objecto de estudo da análise, os «alvos», que alteraram substancialmente as necessidades de *intelligence*.

Até ao fim da guerra fria os «alvos» tradicionais eram os Estados, enquanto que actores não-estatais ou transnacionais eram «alvos» secundários. Na actualidade a prioridade dos «alvos» alterou pelo que a forma de gerar conhecimento terá, necessariamente, de se adaptar à nova realidade, o que levanta alguns desafios.

Assim, o primeiro prende-se com a partilha de *intelligence* e o debate entre a análise competitiva e a análise cooperativa, dos elementos do sistema.

Uma das principais alterações que o novo paradigma de segurança dos Estados veio ressalvar foi a necessidade de partilha de *intelligence* que "at the national or strategic level remains elusive*"* (Kiras, 2007: 145). James Kiras aborda esta temática nos EUA, contudo prossegue afirmando que a falta de cooperação se deve a um conjunto de factores burocráticos e organizacionais, pelo que "are common to almost all democratic governments with large bureaucracies*"* (2007: 145). De acordo com aquele autor, numa perspectiva organizacional as agências competem entre elas para estabelecer e manter a primazia[97] dos papéis em missões específicas, de acordo com o estabelecido na lei, enquanto a regulamentação determina qual a agência que lidera e possui «comando» sobre as outras. De certo que a competição burocrática introduz deficiências no sistema às quais não ficam imunes a eficiência e a eficácia. Estas deficiências incluem, para Kiras (2007: 145), perda de tempo, perda de oportunidades, bases-de-dados incompatíveis, sistemas de classificação e partilha de dados próprios e desperdício de recursos. Ocorrem, por norma, em virtude de «choques de personalidades», suspeição acerca dos motivos e agendas de outras agências, o aumento de autoridade entre agências e a fricção entre agências que possuem capacidades similares ou redundantes, entre outras.

De forma a dar resposta a estes constrangimentos em várias as comunidades de *intelligence*, como a dos EUA, assume-se que o conceito de análise competitiva – possuir diferentes agências, com diferentes pontos de vista a trabalhar o mesmo problema – possui vantagens. De facto, todos os elementos do sistema possuem forças e, provavelmente, pontos de vista diferentes, no que diz respeito

[97] Esta primazia, de acordo com Kiras (2007: 145), está ligada aos recursos fiscais disponíveis para o desempenho de determinada missão.

a diversos assuntos que, ao analisar isoladamente uma determinada situação, podem garantir uma análise mais sustentada e precisa. Contudo, para que tal seja possível é necessário, segundo Lowenthal, que todos os elementos do sistema possuam analistas suficientes, com as mesmas áreas de especialização, o que na actualidade se pode tornar incompatível com os desideratos de eficiência que os decisores assumem. Para além do mais, de acordo com aquele autor, essa redundância de meios, pode à primeira vista ser mais dispendiosa que intelectualmente produtiva tornando-se difícil de sustentar, até porque a maioria dos decisores "cannot abide having agencies disagree, thus vitiating the concept of competitive analysis*"* (2006: 136).

Do outro «lado» da discussão estão os adeptos da análise cooperativa e da criação de centros de análise de *intelligence*. Esta é uma realidade que os EUA conhecem desde os anos noventa do século XX, que a comissão 9/11 recomendou após os atentados de 11 de Setembro, naquele país, de modo a incrementar a análise, *all-source,* regional ou funcional (Lowenthal, 2006: 124-125). Todavia, à semelhança de outras formas de organização, a análise dos SIN não está isenta de algumas fragilidades. A primeira é que esta aproximação torna-se de alguma forma inflexível. Á semelhança de outras burocracias "centers do not like to share or lose resorces" (Lowenthal, 2006: 125) tornando a agilidade analítica mais difícil de alcançar. Decorrente da anterior, os centros tendem a tornar-se competidores, por recursos, com os gabinetes de análise das agências, que não pretendem ver os seus analistas fora do seu controlo e dos quais não recebem resultados directos. De mais a mais, os centros podem vir a garantir conhecimento, com base em análises técnicas, divorciando a informação do contexto político, já que é composto por peritos que tendem a ser especialistas num determinado assunto e não em contextos regionais ou nacionais. Por fim, as questões relacionadas com a tutela dos centros. Que, se estiverem co-localizados com determinada agência, as questões relacionadas com a disponibilidade dos meios é, ainda, mais notória, uma vez que existe o perigo das outras agências perderem aqueles meios durante a prestação de serviço no centro.

Não existe uma forma óptima de organizar a função análise num SIN. Cada esquema possui vantagens e inconvenientes. De acordo com Lowenthal (2006: 126), o objectivo deverá ser o de garantir que analistas – regionais ou especialistas – são chamados a dar o contributo se for caso disso, o que Treverton refere como a gestão matricial[98], que gera a simultaneidade da análise (2009: 153). Em suma, seja de forma permanente ou temporária é crucial garantir a agilidade e a flexibilidade evitando "to hold back the most sensitive and exiting reports until the leaders have been able to deliver the reports to senior policy officials, thus highlighting the skill and cleverness of their people and scoring «points» with the officials*"* (Hulnick, 2006: 963), de modo a impedir o sucedido no referente

[98] De acordo com Chiavenato (2004: 529-531) a essência da gestão matricial é a de combinar as duas formas de departamentalização – funcional e de produto – tratando-se, por isso, de uma estrutura híbrida. "Assim, a estrutura matricial funciona como uma tabela de dupla entrada" (Chiavenato, 2004: 530). Procura tornar a estrutura funcional mais ágil e flexível às mudanças.

aos atentados do dia 11 de Setembro de 2001 em que a *intelligence* "that was critical to informed decisionmaking was not shared among agencies*"* (Kean, 2004: 321). Este ponto sugere que à semelhança da pesquisa a integração e partilha de conhecimento é outro ponto fundamental.

Outro dos desafios que se coloca à função análise é a ligação aos consumidores, uma vez que a análise deve ser entendida como um processo contínuo e integrador. Fruto da fluidez do ambiente, a ligação com os consumidores assume especial importância. Primeiro, porque garante que o produto é percebido pelos que o irão utilizar, possibilitando ao consumidor a criação e teste de variadas hipóteses. Em segundo lugar, porque permite um ganho de tempo que pode ser alocado para a análise da informação. Para Treverton (2009: 164) a prática da análise, na actualidade, é a de que se consome muito tempo a elaborar e a coordenar documentos finais – o produto – ao invés de ter esse recurso alocado ao processo de raciocínio, gerador de conhecimento. Pelo que, ao empenhar o decisor no processo de análise poupa-se tempo que pode ser alocado ao processo de raciocínio.

No quadro da disseminação, surge, no século XXI, uma nova realidade, A necessidade de conhecer por parte de outras entidades que não os decisores políticos e militares. Treverton (2009: 185) sistematiza-os em oito novos tipos de utilizadores de *intelligence*: (*i*) comandantes militares tácticos; (*ii*) agências federais «domésticas»; (*iii*) Organizações Não-governamentais (ONG); (*iv*) conjunto alargado de agências federais; (*v*) autoridades locais e estaduais; (*vi*) órgãos de polícia; (*vii*) gestores privados de infraestruturas públicas; (*viii*) cidadãos privados. Sendo que as primeiras três categorias surgem no período anterior ao 11 de Setembro e à, designada, guerra global contra o terrorismo.

A primeira categoria ainda que coincida com o fim da guerra fria, não decorre daquele conflito. De facto, o empenhamento militar no Teatro de Operações da Europa, em operações de apoio à paz, na região dos Balcãs, permitiu que os sistemas de TECHINT – SIGINT e IMINT – antes designados para compreender a URSS, fossem redireccionados para apoiar os comandantes militares tácticos[99]. A mesma tipologia de operações militares e outras operações de contingência facilitou o desenvolvimento de ONG, muitas vezes em áreas do globo que não haviam sido a prioridade de *intelligence* para os Estados ocidentais. No entanto, por natureza, estas organizações são cépticas relativamente aos governos e, em particular, relativamente às agências de *intelligence*. No entanto, de acordo com Treverton "they also eventually welcomed the idea that someone cared about their issues*"* (2009: 186)[*100*]. A segunda categoria é resultado do final da guerra fria. A globalização da economia mundial, após 1989 abriu espaço para necessidades de *intelligence*, ao nível do departamento de comércio, nos EUA, e dos seus congéneres, noutros Estados. A informação económica pauta-se, essencialmente, por uma premência grande em termos de oportunidade. Traduz num enorme desafio para os SIN. Neste sentido, a pressão exercida sobre as agências de *intelligence* aumentou de forma

[99] O apoio dos satélites, em termos de comunicações seguras, a identificação positiva de alvos, etc.
[100] Esta ideia é sustentada no facto de que ao nível do terreno as forças militares operarem os Civil-Military Co-operation Centers (CMOC).

significativa. Por um lado, mais utilizadores, por outro, menos meios. O que afecta, de forma substancial, a capacidade de conduzir análises profundas.

As restantes cinco categorias de utilizadores são produto dos atentados de 11 de Setembro de 2001. No combate ao terrorismo o esforço deve recair na prevenção, o que implica que é, para Treverton (2009: 186), um conflito, essencialmente, de *intelligence.* A lógica da prevenção é impedir que os terroristas possam operar. Nesse sentido, surgem uma série de agências do Estado[101] que passam a estar empenhados neste conflito e necessitam de *intelligence* para se tornarem parte da solução. Ainda que as necessidades variem de agência para agência, numa perspectiva de *latu sensu* as necessidades são estratégicas e tácticas[102]. A mesma necessidade é manifestada pelas forças de polícia. Contudo, deve ter-se em consideração o espaço de jurisdição daquelas forças, de forma a adequar a *intelligence* às reais necessidades[103]. O sector privado é outra das categorias cujas necessidades surgem desde 11 de Setembro. Muitas das infraestruturas públicas são geridas pelo sector privado como por exemplo o sector da informação, o sector financeiro e os transportes. A informação de que necessitam deverá ser, idealmente, talhada a cada sector em particular. Primeiro, porque prestam serviços públicos à população e no caso de pararem os constrangimentos são enormes para a sociedade[104]. Depois, são, para Treverton (2009: 187), símbolos da sociedade ocidental, consequentemente um objectivo para grupos terroristas[105]. Por fim, o cidadão privado que para além de necessitar de conhecer a ameaça, deve ter conhecimento de forma a identificar indícios e, acima de tudo, ter consciência de como deve reagir, caso seja necessário.

Contudo, as alterações de paradigma são difíceis de operacionalizar. A *intelligence*, produzida pelas várias agências está sujeita a protocolos de segurança, o que em larga medida dificulta a partilha entre as agências de um SIN. A este propósito Hulnik (2006) refere que o factor que afecta a confiança e uma análise integrada entre as diversas agências de um SIN é, acima de tudo, a ligação e partilha de informação entre agências. Segundo aquele autor, há uma tendência natural para que as diversas agências se centrem em demasia no paradigma do *need to know*. Para além do mais, se entre agências de *intelligence* de um SIN é difícil a partilha, muito mais se tornará quando se fala em consumidores que estão fora dos canais de disseminação, normais, dos SIN. No entanto, essa partilha pode ser o suficiente para impedir um ataque de, por exemplo, um grupo terrorista como os ocorridos nos EUA, Espanha ou Londres. Para isso há que partilhar a informação com quem tem necessidade de conhecer

[101] Desde o controlo de fronteiras aos centros de controlo médico.

[102] Por exemplo, o controlo de fronteiras (que no Espaço *Shengen* é mais complexo) necessita de ter um conhecimento, estratégico, dos eixos de infiltração de grupos trans-nacionais e, no âmbito táctico, de indícios acerca de comportamentos suspeitos.

[103] Por exemplo, em Portugal, Distritos de fronteira terrestre (por exemplo Bragança ou Castelo-Branco) têm necessariamente necessidades estratégicas e tácticas diferentes dos Distritos do litoral, como Lisboa ou Porto.

[104] Por exemplo se a rede de transportes deixar de funcionar vários sectores são afectados, como por exemplo a economia.

[105] Veja-se os atentados das torres gémeas, em Nova Iorque, ou do metro, em Madrid, entre outros.

e, acima de tudo, em tempo, pelo que a antecipação passa necessariamente pela identificação, em tempo, do utilizador que tem necessidade de aceder a essa informação, de modo a evitar ocorrências catastróficas.

3.3. A Counterintelligence

A *couterintelligence*, é a função da *intelligence* que tem como principal racional a protecção das capacidades de *intelligence* contra as actividades de *intelligence* hostis. O seu objectivo é a degradação das capacidades de pesquisa e análise de *intelligence* do adversário. Primeiro, porque nega o acesso do adversário a determinada informação, através da segurança e contra-espionagem. Em segundo lugar, através das operações de decepção introduz *inputs* falsos ou informação deliberadamente enganadora para que os sistemas adversários cheguem a conclusões incorrectas acerca das capacidades, intenções e acções em relação ao seu «alvo».

Das funções da *intelligence* a *counterintelligence* (CI) é, provavelmente, de acordo com autores como Lowenthal, Shulsky e Schmittd, das mais difíceis de caracterizar. É, à semelhança da *intelligence*, simultaneamente um produto e uma actividade. Produto, na perspectiva de que é informação fidedigna acerca de sistemas hostis e outras ameaças ao Estado. Pelo que, necessita conhecer a estrutura organizacional, do adversário, o seu pessoal-chave, métodos de recrutamento e treino e detalhes de operações específicas. Como actividade, Shoulsky e Schmitt identificam as medidas passivas e activas (2002: 99).

As primeiras, procuram negar o acesso dos sistemas hostis à informação, as segundas, procuram perceber como os SIN hostis funcionam, de forma a frustrar ou a disromper as suas actividades e, em última análise, tornar as actividades hostis numa vantagem para o próprio SIN.

Das medidas passivas fazem parte os sistemas de classificação da informação e as medidas de segurança. Os sistemas de classificação de informação têm por racional a categorização da informação de acordo com a sua sensibilidade[106]. Quanto mais sensível a informação mais cuidado se deve ter no seu manuseamento e, consequentemente, menor o número de pessoas com o grau de credenciação[107] que lhes permite manusear tal informação. Contudo, o grau de credenciação não é suficiente para obter o acesso à informação. Nesse sentido, é estabelecido um sistema de controlo informal, o princípio do *need to know*[108] que permita, aos elementos que necessitam, aceder à informação necessária ao cabal desempenho das suas tarefas oficiais (Shulsky e Schmitt, 2002: 99-100).

---

[106] Neste contexto podemos associar a sensibilidade da informação ao dano que a revelação da mesma, a um poder hostil, poderá causar ao Estado. Por exemplo, o grau de «muito secreto» - danos excepcionalmente graves; «secreto» - danos sérios; «confidencial» - danos (Shulsky e Schmitt, 2002: 100).

[107] Grau de autorização, formal, para aceder à informação sensível (Shulsky e Schmitt, 2002: 100).

[108] Este sistema de controlo informal garante, para Lowenthal, a compartimentação do sistema uma vez que, apesar da credenciação um analista que trabalhe com fontes, por exemplo IMINT, pode encontrar dificuldade em aceder a informação proveniente de fontes de HUMINT (2006: 148-149)

Apesar das vantagens que o sistema de classificação de informação apresenta, num contexto de segurança, o mesmo representa alguns custos em termos de flexibilidade e integração. Primeiro, porque favorece a burocratização do sistema, dificultando a flexibilidade. Depois, porque, de acordo com Lowenthal (2006: 149), ao limitar a informação a análise pode encontrar obstáculos inerentes à exclusão do acesso a informação crucial para o desenvolvimento das suas tarefas.

As acções de segurança são aquelas que permitem a obstrução da capacidade de pesquisa de uma ameaça hostil. São desenvolvidas no sentido de prevenir o acesso, a exploração do acesso a pessoal, documentos, comunicações ou operações, de modo a ter ganhos de informação. Constituem-se, por isso, como «barreiras» que delimitam a informação classificada (Shulsky e Schmitt, 2002: 105). Destas fazem parte as medidas de segurança pessoal e segurança física.

As primeiras envolvem procedimentos para a despistagem[109] de potenciais funcionários, antes da sua contratação, e de garantia que os actuais mantêm os padrões de confiança desejáveis, as designadas investigações de segurança. Os elementos chave desta avaliação são a lealdade e o carácter do funcionário ou potencial funcionário. Sendo, para o efeito, desenvolvidas investigações de segurança (Shulsky e Schmitt, 2002: 105). Por segurança física podemos entender as acções desenvolvidas para prevenir agentes hostis de obterem o acesso físico à informação classificada. Lida, essencialmente, com assuntos como as características de cofres e de sistemas de alarme para a detecção de intrusão.

Das medidas activas de CI podemos identificar, de acordo com Shoulsky e Schmitt (2002: 108), três actividades principais: a contra-espionagem; a CI multidisciplinar; e a decepção e contra-decepção.

A primeira procura frustrar as actividades hostis, utilizando para o efeito operações de vigilância e o uso de agentes duplos ou dissidentes.

Com as operações de vigilância pretende-se, acima de tudo, determinar rotas, contactos e com quem os agentes hostis comunicam. No entanto, embora conceptualmente simples, torna-se de difícil operacionalização. De acordo com Wettering (2010: 293-294) este tipo de operações pode recorrer a três técnicas: a vigilância estática[110]; vigilância móvel[111]; por fim, as vigilâncias electrónicas[112].

O segundo método, o uso de agentes duplos[113] ou dissidentes permite a penetração nos mecanismos

[109] a principal função dos procedimentos de despistagem é o de avaliar a habilidade e vontade dos potenciais ou actuais funcionários em materem a informação classificada em segredo.

[110] Um local de onde se pode observar o «alvo», de modo a permitir alertar equipas de vigilância móvel, identificar padrões de comportamento do «alvo» e contactos e identificar contactos nas embaixadas.

[111] Efectuada de modo a intimidar e desencorajar suspeitos de conduzirem actividades ilegais relacionadas com a espionagem e capturar suspeitos de espionagem em flagrante

[112] Com recurso a escutas ou outros meios de intercepção (com recurso às capacidades de COMINT) que shoulsky e Schmitt consideram CI multidisciplinar (que será debatido posteriormente).

[113] Agentes que enquanto supostamente operam para um sistema hostil, estão sobre o controlo do Estado que deveriam estar, supostamente, a espiar.

do adversário e a identificação de agentes de SIN hostis, empenhados na gestão de fontes. Para além de identificar elementos hostis, este tipo de operações, permite aos elementos de CI aprender acerca dos métodos operacionais dos seus adversários e das prioridades de *intelligence* adversárias. Assim, ao saber quando e como os adversários comunicam com as suas fontes, mais facilmente a CI pode contrariá-los. Para além do mais, o conhecimento acerca do adversário contribui para a CI identificá-lo, bem como ao equipamento com que opera. Este método de pesquisa tem como alvo o SIN adversário ao invés das lideranças políticas, militares ou outras, próprias da função pesquisa. É o "the most direct way to achieve counterespionage goals is to collect intelligence directly from the hostile service, either by human or technical means"[114] (Shulsky e Schmitt, 2002: 109).

A CI multidisciplinar tem como enfoque contrariar as ameaças que um adversário, com recursos tecnologicamente desenvolvidos, coloca.

Actualmente, as capacidades de pesquisa de *intelligence* dos vários Estados não são apenas relegadas à HUMINT, pelo que as actividades de CI devem ter em consideração as capacidades de TECHINT, adversárias. Nesse sentido, a primeira tarefa da CI multidisciplinar é a de identificar as capacidades de pesquisa TECHINT do adversário para poder, posteriormente, avaliar as, próprias, vulnerabilidades, seja em termos de comunicações, seja no que respeita a actividades, e assim melhor protegê-las. Estas medidas podem ser designadas de «contramedidas técnicas» e variam de acordo com a tecnologia. A perspectiva multidisciplinar permite vislumbrar o problema sobre a perspectiva da ameaça, ou seja, ter em consideração as capacidades totais do adversário e de que forma pode operar de forma sinérgica (Shulsky e Schmitt, 2002; 114-116).

Nas duas medidas, anteriormente descritas, o enfoque é colocado na negação do acesso à informação por parte das capacidades de pesquisa de *intelligence* adversárias, que quando efectuadas com sucesso levará a uma presumível falta de informação. A decepção é a tentativa de induzir em erro a função análise e pesquisa do sistema adversário[115] que, formando uma imagem errada da situação, procura levar as suas lideranças a agir em consonância com os interesses da outra parte. Esta medida é considerada, para Shulsky e Schmitt (2002: 117), uma forma de CI porque procura distorcer o fundamento das operações de *intelligence* adversária. Para além do mais, recorre métodos de CI como as operações com agentes duplos. O racional desta medida é o de bloquear a recepção dos sinais tidos como verdadeiros[116] e substituí-los por «realidades alternativas». Se a primeira parte do processo é uma questão de segurança – através do conhecimento abrangente dos canais de recepção adversários –

[114] A título de exemplo temos o caso Kim Philby (agente do MI 6) que, após a segunda guerra mundial, informava o KGB das operações cobertas americanas e britânicas na Ucrânia, Rússia e Albânia, tendo, assim comprometido inúmeros agentes americanos e britânicos ou o caso de Oleg Gordievsky, vice-embaixador soviético, em Londres, que, nos anos oitenta, informava o MI 6 e o MI 5 das «toupeiras»[114] (Shulsky e Schmitt, 2002: 109-110).

[115] No que concerne à situação política, militar e económica, por exemplo.

[116] Os que reflectem as actividades actuais.

a segunda – criação de sinais falsos – pode envolver o uso de agentes duplos, que disseminarão a informação falsa através dos canais anteriormente identificados. No entanto, para que produzam efeitos, os esforços de decepção têm de ser plausíveis, isto é "success is more likely if the deception scenario is based on what the adversary thinks is the case*…"* (Shulsky e Schmitt, 2002: 121). Pelo que, os sinais criados para induzir o adversário em erro devem reforçar o ponto de vista, errado, e prevenir que quaisquer sinais verdadeiros possam afectar tais percepções, evitando a contra-secepção adversária[117].

3.4. A acção coberta

A acção coberta (AC) tem por objectivo disromper o processo de decisão política dos decisores adversários. Independentemente da forma como se pressente sobressai que o cerne desta actividade é a influência directa no processo de decisão política. Pelo que sendo uma das actividades de *intelligence* difere, conceptualmente, das outras funções.

Se as anteriores têm como preocupação a procura e a salvaguarda da informação, a AC procura a influência nos eventos políticos. Nesse sentido, Steiner citado por O'Brien refere que a AC "is all about making things happen, while intelligence consists of making the right decisions about what to make happen*"* (2007: 25). Para além do mais, Godson citado, também, por O´Brien ao fazer a distinção entre CI e AC menciona que a CI é focada nos operacionais de *intelligence* e nos decisores políticos, enquanto a AC tem como «alvo» "non-intelligence players*"* (2007: 25).

É frequentemente designada de *quiet option*, seja em termos de actividade de *intelligence*, seja no contexto das RI. Ainda que usada ao longo da história da humanidade, formalizou-se e burocratizou-se, enquanto actividade de *intelligence* durante o século XX. Atingiu o ponto alto no período da guerra fria, tendo sido usada por ambos os blocos antagonistas na prossecução dos seus interesses geopolíticos (O'Brien, 2007: 23). No entanto a guerra fria não pôs um fim a esta actividade. De acordo com O'Brien, na actualidade, tal como durante a guerra fria, e antes, a AC "continues to be a tool used to support states' interests and rivalries around the world" (2007: 24).

O âmbito da AC é bastante abrangente. Johnson e Wirtz (2004: 253) designam-na de *third option* – uma opção firmada entre a diplomacia e a guerra. Seguindo o mesmo racional Godson (1995: 156) transmite a ideia de que são as acções efectuadas por um governo para influenciar eventos, noutro Estado ou território, sem revelar o seu envolvimento. O'Brien (2007: 24) acrescenta que é a sua natureza coberta que permite aos Estados utilizá-la quando a primeira, a diplomacia, é insuficiente para atingir os objectivos e, a segunda, o emprego de forças armadas não é opção. Para além do mais,

[117] A contra-decepção tem por objecto determinar o risco do sistema se tornar alvo de decepção e mitigá-lo de forma a proteger a integridade das próprias operações de *intelligence.*

a natureza coberta garante a «negação plausível»[118], ou seja, que o Estado opere fora do seu território sem que a sua presença seja conhecida ou notada.

Para Johnson e Wirtz (2004: 254-259), bem como para outros autores como O'Brien (2007: 25) as categorias de acção coberta são quatro: (*i*) propaganda; (*ii*) acção coberta política; (*iii*) acção coberta económica; (*iv*) acção paramilitar.

A primeira é, para Lowenthal (2006: 162), a mais antiga técnica de disseminar informação com o objectivo de um *outcome* político específico. É entendida por Janowitz *apud* (O'Brien, 2007: 33) como a disseminação planeada de notícias, informação, argumentos e apelos especialmente desenhados para influenciar as crenças, opiniões e acções de um grupo específico ou de um indivíduo. Focada em actividades efectuadas de forma aberta ou coberta, esta técnica é, por norma, utilizada em conjunto com outras técnicas[119]. Pode ser utilizada para o apoio de indivíduos, grupos amigáveis, exaurir o poder de adversários, criar falsos rumores de agitação política, capitalizar a escassez económica ou ataques directos a adversários[120]. O principal objectivo da propaganda é a persuasão[121].

A acção coberta política é apresentada por Lowenthal (2006: 162) como a forma das operações de *intelligence* intervirem mais directamente no processo político do Estado-alvo. Envolve, para Godson (1995: 156), o apoio e coordenação de agentes de influência e outros envolvidos nos mais altos círculos políticos, podendo, no entanto, extender-se a campos não-governamentais como sindicatos, movimentos juventude, círculos intelectuais e movimentos religiosos, por exemplo. Tal como na categoria anterior pode ser empregue para apoiar aliados ou para impedir ameaças de concretizarem os seus objectivos[122].

A acção coberta económica é a terceira categoria. Inclui tentativas, através de meios cobertos, de disromper ou destabilizar as economias adversárias. Para o efeito, de acordo com O'Brien (2007: 42-43), utiliza métodos como contrafacção de moeda estrangeira, abaixamento dos preços, nos mercados mundiais, das *commodities*[123] vitais ao adversário[124], destruição de linhas de abastecimento eléctrico,

---

[118] *Plausible deniability*, que segundo Lowenthal (2006: 166) é um conceito central à acção coberta. Procura transmitir a ideia que se o envolvimento de um Estado, em actividades de acção coberta, for conhecido o chefe de Estado pode negar o seu consentimento nessa acção. Pode, inclusivamente, afirmar, com alguma plausibilidade, que a acção foi desenvolvida pelos seus subordinados sem o seu conhecimento ou autoridade (Shulsky e Schmitt, 2002: 93).

[119] Por exemplo, acção coberta política

[120] Como exemplo temos as «fugas» de informação para jornais, ou outros meios de *media* do Estado-alvo.

[121] Neste sentido O'Brien (2007: 33) refere que a persuasão pode ser uma mistura de ameaças e apelos que incluem um largo elemento de coacção física e psicológica. Pode incluir chantagem, subornos e ameaças de aplicação de actos de violência física como raptos e torturas, por exemplo.

[122] Utiliza vários métodos, onde os pagamentos secretos a políticos, burocratas ou a partidos políticos estrangeiros, são um exemplo e o apoio à eclosão de manifestações e interferência com as promulgações da ameaça, são outro.

[123] Usada como referência às matérias-primas ou produtos com pequeno grau de industrialização, de qualidade quase uniforme, produzidos em grandes quantidades e por diferentes produtores (e.g. ferro, ouro, petróleo, trigo, milho, café, entre outros)

[124] Principalmente àqueles estados que dependem da produção de uma única matéria prima

destruição de portos marítimos, entre outros. De acordo com Johnson e Wirtz em virtude da dependência económica, financeira e informática "with skillful hacking (cyberwarfare), a nation or group's financial transactions can be left in disarray, its bank assets stolen (…) an electronic assault that could be at least as dislocating as a military attack*"* (2004: 257).

A última, a acção paramilitar, é considerada por Johnson e Wirtz (2004: 257) a categoria cujo uso da violência é notório e, por isso, representa uma maior controvérsia. Godson (1995: 157) apresenta o apoio a grupos terroristas, movimentos insurgentes ou outro tipo de grupos não convencionais, bem como o apoio a forças governamentais que contrariem a acção destes como alguns exemplos desta actividade. O´Brien (2007: 43-47) acrescenta, ainda, todas as formas de assassinato[125] de indivíduos estrangeiros[126] e golpes de Estado. Para aquele autor o cerne desta categoria é a violência armada pelo que, todos os actos que sejam conduzidos num contexto de acção coberta, cuja natureza seja a violência armada, deve ser considerado como acção paramilitar.

Ao vislumbrar as categorias desta actividade fica a ideia de que é discutível considera-la uma actividade de *intelligence*, nascendo, por isso, o debate em torno desta problemática. Um dos pólos alimenta a discussão argumentando com o provável enviesamento da análise da *intelligence,* já que se está a atribuir as responsabilidades de implementação de política, de pesquisa e análise de *intelligence,* incluindo a análise dos efeitos da acção coberta, à mesma agência (Shulsky , 1995: 94). O outro pólo contra-argumenta que as agências de *intelligence* são as organizações que devem conduzir esta actividade. Primeiro, porque a história demonstra que se existirem organizações separadas[127] pode gerar-se falta de coordenação e disputa de recursos, conduzindo a resultados catastróficos[128] (Shulsky e Schmitt, 2002: 95). Em segundo lugar, porque ainda que, conceptualmente, a acção coberta e a pesquisa HUMINT sejam diferentes, ambas dependem recursos similares, principalmente na cooperação secreta de agentes habilitados a operar no Estado-alvo. De acordo com Shulsky e Schmitt (2002: 95), na maioria dos casos os agentes que desenvolvem uma das funções podem desempenhar a outra. Para além do mais, as tarefas[129] desempenhadas para apoiar ambas as funções requerem competências, contactos e recursos similares.

Em suma, apesar do debate em torno da validade da AC enquanto actividade de *intelligence*, importa salientar que a noção de *intelligence* ficaria incompleta ao cingir, apenas, à obtenção de informação e decorrente conhecimento. Assim, se a obtenção de *intelligence* é tão importante, a sua negação também o é e uma das formas de negar a verdade ao adversário é criar decepções e induzi-lo em erro. A AC, tal como a CI garantem esse desiderato, para além de que pode, através de alguns

[125] Johnson e Wirtz (2004: 258) identificam o assassinato como outra categoria da acção coberta.
[126] Por vezes designado de *target killing.*
[127] Uma dedicada às actividades de pesquisa e segurança da *intelligence* e outra dedicada, em exclusividade, à acção coberta
[128] Tendo como base a experiência americana e britânica da II guerra mundial.
[129] Assegurar as comunicações entre agentes e gestores de fontes ou pagamentos clandestinos.

métodos[130] paralisar a acção adversária e, assim, disromper, ainda que momentaneamente, o seu ciclo de decisão. Importa ainda, vincar, que a AC não é um substituto da política externa. É, para Godson, "gererally counterproductive when used by a government that has not really decided what it wants to do, but wants to do something" (1995: 167). De mais a mais, a CA é um dos instrumentos que pode ser usado quando é claro que os objectivos do Estado não podem ser atingidos, exclusivamente, por ou tão eficazmente com recurso a meios abertos, por via da diplomacia ou emprego da força armada.

[130] Por exemplo o *target killing*, subornos ou chantagem, entre outros.

> *"…os Romanos fizeram aquilo que todos os príncipes sábios sabem fazer, isto é, não só fazer face às questões do presente como prevenir (…) as que podiam sobrevir no futuro, porque, antecipando a sua ocorrência, facilmente se podem remediar."*
>
> Nicolau Maquiavel[131]

CAPÍTULO IV – A EFICÁCIA

A noção do conceito de eficácia está directamente relacionada com a concretização dos objectivos e com os resultados pretendidos. Chiavenato apresenta-nos esta noção como sendo "*uma medida do alcance de resultados, ou seja, a capacidade de atingir objetivos e alcançar resultados (…) Relaciona-se com os fins almejados"* (2004: 183) centra-se nos *outputs* dos processos. Assim importância desta noção, no contexto da *intelligence*, é central para se obter e manter uma capacidade credível no âmbito da redução da incerteza. O conhecimento gerado é um *input* do processo de decisão. Nesse sentido, o conhecimento pode permitir a obtenção de vantagem sobre o oponente ao garantir a rentabilização[132] dos meios do Estado, alocados à implementação da acção política, de modo a obter vantagem sobre o oponente.

Contudo, a grande dificuldade está na medição, objectiva, dos *outputs* da *intelligence.*

A *intelligence* é condição suficiente[133] para que o processo de decisão se efectue. O que implica que, ainda que sem o conhecimento facultado pelas organizações de *intelligence*, o processo de decisão pode ser realizado. De acordo com Mintz e DeRouen (2010: 38) os decisores tendem a ver o mundo de uma forma própria[134] filtrada de forma subconsciente por crenças e experiências anteriores levando-os, por vezes, a desvirtuar a decisão. Nesse sentido, aqueles autores, apresentam *"*ignoring critical information*"* (2010: 39), entre outras, como uma das formas de demonstrar o referido viés no processo de decisão.

Depois, o facto do resultado do processo, conduzido pelas organizações de *intelligence*, ser um intangível incrementa, de sobremaneira, os obstáculos à medição da concretização do produto final. Primeiro, a qualidade das decisões não é, necessariamente, directamente proporcional à qualidade dos *inputs*, que as organizações de *intelligence* facilitam. Depois, a qualidade da *intelligence* nem sempre é garantida, podendo em determinadas situações induzir as elites decisoras em erro, o que concorre,

---

[131] Maquiavel, Nicolau (2007). O Príncipe, Lisboa, Edições Sílabo. (pp. 49-50).

[132] A procura pela eficiência, que Chiavenato define como "… uma relação entre custos e benefícios, entre entradas e saídas, ou seja, a relação entre o que é conseguido e o que pode ser conseguido. Significa fazer corretamente as coisas e enfatizar os meios pelos quais elas são executadas. Relaciona-se com os meios, isto é, com os métodos utilizados" (2004: 183).

[133] De acordo com Freitas (1989: 1094) a condição é suficiente quando é requerida para "qualquer coisa exista, mas não é absolutamente necessária*"*; ainda de acordo com aquele autor, a condição é necessária quando é indispensável.

[134] O que se designa de factores psicológicos.

substancialmente, para a falta de comunicação entre decisores e SIN.

4.1. O ciclo de decisão em política externa

Quando falamos de decisão em política externa, estamos a referirmo-nos às escolhas de indivíduos, grupos e coligações que afectam as acções do Estado no palco internacional (Mintz e DeRouen, 2010: 3). As quais são caracterizadas como de envolver "high stakes, enormous uncertainty, and, as result of these elements, substantial risk*"* (Renshon e Renshon, 2008: 509).

Para Mintz e DeRouen, muito do que se pressente no contexto internacional prende-se, essencialmente, com as acções dos Estados e dos seus líderes. De acordo com aqueles autores "the course of politics is shaped by leader's decisions" (2010: 4). O que, quando o tempo para a tomada de decisão é escasso, os riscos são altos e há incerteza acerca dos motivos, crenças, intenções ou cálculos do oponente, pode levar a que seja difícil obter "*high-quality decisions*" (Renshon e Renshon, 2008: 514), obrigando os decisores a agir por instinto[135]. No entanto os factores psicológicos, anteriormente descritos, associados aos líderes são apenas um dos determinantes que enformam a decisão em política externa. Nesse sentido, Mintz e DeRouen (2010: 4) assumem, para além dos anteriores, o ambiente em que a decisão se desenvolve, os factores internacionais e os factores domésticos como os principais factores que determinam os *outcomes* na decisão em política externa. Segundo os mesmos autores, a essência da maioria das decisões em política externa é a de um processo de decisão que ocorre de forma interactiva e consiste numa sequência de decisões, tomadas sobre a pressão do tempo. Citando Robinson e Snyder, Mintz e DeRouen (2010: 4) referem que a decisão em política externa consiste em quatro componentes: (*i*) identificar o problema de decisão; (*ii*) procurar alternativas; (*iii*) escolher a alternativa; (*iv*) execução da alternativa.

Esta perspectiva encontra paralelismo na tese apontada por John Boyd, através do seu ciclo de decisão que prevê, também, quatro componentes, o ciclo OODA: (*i*) observar; (*ii*) orientar; (*iii*) decidir; (*iv*) agir. Boyd assume que o ciclo OODA "suggests that the process of observation, orientation, decision and action is a circular, iterative process" (Osing, 2007: 5). Pelo que podemos inferior que os quarto components apresentados por Mintz e DeRouen podem interagir da mesma forma que o ciclo OODA, de Boyd. Definindo-se, assim, um ciclo de decisão, na política externa, composto por aqueles componentes (conforme figura IV.1).

[135] Para Renshon e Renshon instinto pode ser entendido, neste contexto, como a sua visão global estratégica, códigos operacionais, preferências heurísticas, estratégias de liderança e tendências psicológicas. Todos estes factores são subjectivos e não têm de ser, necessáriamente, errados. Mas são, por certo inconsistentes com o modelo do actor racional. (2008: 514).

Figura IV.1 - Ciclo de Decisão, adaptado de Mintz e DeRouen (2010: 4)

O primeiro componente, a identificação do problema prende-se, essencialmente, com o acesso à informação relativamente ao ambiente, capacidades, intenções e métodos. Aquela informação que permite mitigar a incerteza que o ambiente coloca. Refere-se à necessidade de escrutínio do ambiente ao coligir informação relevante e determinar as circunstâncias sob as quais se deve operar. É a fase designada por Herbert Simon, *apud* Mintz e DeRouen (2010: 17), como *intelligence,* onde prevê a pesquisa de informação e a identificação do problema.

O segundo componente, procurar alternativas, assume a necessidade de efectuar estimativas, identificar pressupostos, analisar e efectuar julgamentos sobre a situação de modo a criar uma imagem mental consolidada. É a compreensão das circunstâncias do ambiente em que se opera. A fase que Herbert Simon designa de esboço – identificar alternativas e seleccionar critérios. Será nesta fase que se elencam os meios disponíveis para a consecução da política externa, que de acordo com José Cavet de Magalhães *apud* Bessa (2001: 136-138), se sistematizam em meios pacíficos e meios violentos. Os primeiros enquadram: a negociação - a matéria que constitui a diplomacia e a mediação que busca um entendimento das partes em conflito; a propaganda – que busca explorar as vulnerabilidades da opinião pública do adversário, enquadra-se nas operações desenvolvidas no quadro da acção coberta; a espionagem – a *intelligence* necessária aos decisores; a pressão económica – visa criar dificuldades ao consumo e vida quotidiana dos cidadãos de um Estado adversário no sentido de forçar a decisão das elites adversárias, se desenvolvida de forma coberta enquadra-se nas operações de acção cobertas; a pressão política – que pretende as mudanças de postura nas decisões das elites políticas adversárias pela aplicação de influências ou chantagem, técnicas associadas à acção coberta. Os segundos envolvem: a dissuasão – a inibição para a acção do adversário através de uma força acumulada,

credível, e conhecida no alcance do seu poder de destruição; a ameaça – na qual se deve representar uma hipótese credível de uso da força, por parte do ameaçador[136]; as pressões económicas – que configuram sanções concretas de cariz económico; a pressão militar – a qual se pode observar através da mobilização acelerada, manobras militares junto das fronteiras, demonstração de força, aquisição de equipamento sofisticado e outros; e guerra.

A terceira, a escolha de alternativas, tem como cerne efectuar a comparação das diferentes alternativas, utilizando os critérios e efectuar a escolha da que melhor se enquadra na solução pretendida. Uma vez a fase de procura de alternativas completa, há a necessidade de ser efectuada a escolha, isto é, decidir entre as alternativas possíveis, tendo em consideração as circunstâncias e os critérios definidos, anteriormente. É a fase de opção preconizada por Herbert Simon.

No quarto componente, a execução da alternativa, pretende-se pôr em execução a decisão tomada anteriormente. Nesta fase serão determinadas as tarefas a desenvolver aos órgãos que a irão implementar, e alocados os recursos para tal. É a implementação de Herbert Simon.

Assim, tendo como base o ciclo de decisão de política externa (ver figura IV. 1) ou o ciclo de decisão de Boyd consegue perceber-se que a vantagem de decisão se consegue desde que a decisão percorra aqueles componentes mais rapidamente que o adversário. E nesse sentido é imperioso o papel da *intelligence* em todas as fases do ciclo ou, utilizando a terminologia de Mintz e DeRouen, nas componentes da decisão em política externa.

Após o debate do ciclo de decisão em política externa fica-nos a percepção que o esforço da *intelligence* é maior na primeira fase e que as decisões, decorrentes das fases subsequentes, serão mais adequadas quanto menos incerteza estiver presente, como resultado da primeira fase. Contudo o papel da *intelligence* deverá acompanhar todos os componentes daquele ciclo.

De acordo com Sims (2009: 62) o racional dos SIN é o de obter vantagem de *intelligence* de forma a garantir a vantagem na decisão, entendendo essa vantagem como a forma de aprimorar a decisão, relativamente ao oponente. Pelo que o teste da *intelligence* é a sua relevância e oportunidade para a decisão. De qualquer forma, obter vantagem de *intelligence* implica conhecimento superior acerca de capacidades, intenções e actividades de outros actores ou criar condições para desestruturar as suas decisões. Seja pela indução da incapacidade de perceber o meio e o, decorrente, problema da decisão, seja pela recorrente necessidade de emendar más decisões. O desequilibrar o adversário.

[136] para isso há que ter em consideração a percepção do poder do adversário, a avaliação da determinação das elites dirigentes e os custos do cumprimento da ameaça, para além destas a personalidade do líder poderá ser outro dos factores a ter conta.

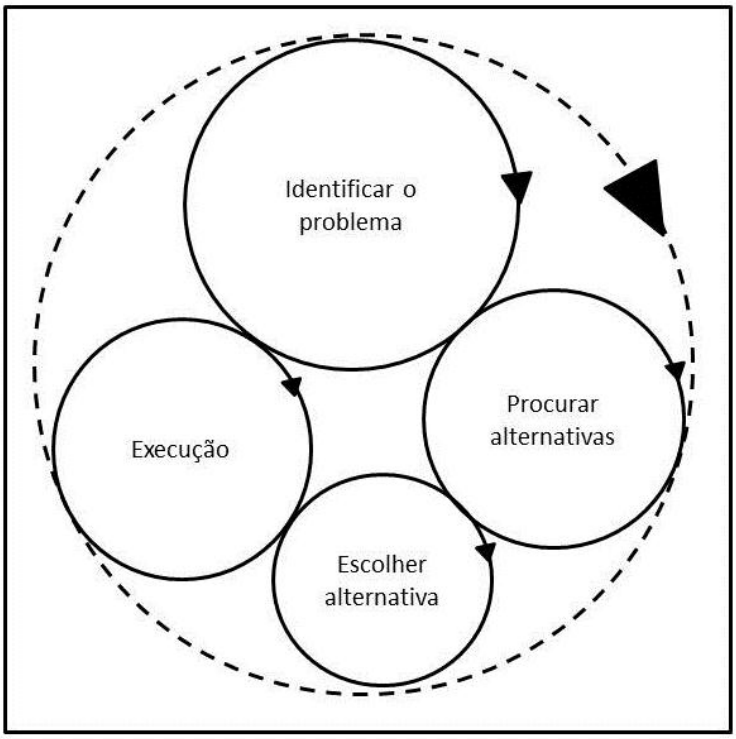

Figura IV.2 - O «peso» relativo da *intelligence* no ciclo de decisão de política externa

Para tal um ciclo de decisão menos amplo que o adversário obrigá-lo-á a reagir e emendar as suas decisões. Tem, então, a vantagem o actor que possuir um ciclo com menor amplitude (conforme figura IV.2). Pelo que, importa que a *intelligence* seja integrada em todo o ciclo de decisão.

Primeiro, porque as deliberações relacionadas com a política externa devem ter início com a "intelligence picture*"* (Gazit, 1989: 269). São as estimativas relativamente às capacidades, intenções e actividades do adversário, para além de identificar as suas possíveis linhas de acção. O que corresponde *latu sensu* à primeira fase do ciclo. Neste sentido, usando as palavras de Michael Warner (2009b: 20), é nesta fase que a *intelligence* opera a transformação da incerteza[137] em risco[138].

Em segundo lugar, na segunda fase, importa salientar que dos vários meios possíveis de empregar, violentos ou não, alguns são actividades desempenhadas pelos SIN, seja pela função pesquisa seja pela função acção coberta. Para além do mais, ao identificar as possíveis opções, os SIN poderão avaliar os possíveis *outomes* de cada opção, que ajudarão na identificação das opções e critérios mais adequados, tendo em vista as intenções dos decisores.

Em terceiro lugar, coincidente com a terceira fase, a influência dos SIN pode manifestar-se através do refinamento dos *outcomes* das opções que serão alvo de escolha, de forma a permitira a seleção daquela que represente menor risco na consecução dos objectivos elegidos por decisores.

[137] Na qual não é possível prever um *outcome* nem a probabilidade de ocorrência.
[138] É possível calcular o impacto e a probabilidade de ocorrência.

Em quarto lugar lugar, na quarta fase após ser determinado quais os elementos que deverão desenvolver actividades no sentido de atingir os objectivos preconizados pelos decisores, os SIN poderão suportar esses órgãos subordinados, com *intelligence*, no sentido de ser mais célere a implementação da decisão. Para além do mais, uma das atribuições dos SIN é a monitorização das reacções do adversário, resultantes da decisão, as quais se necessário garantem com a necessária oportunidade *intelligence* relevante para alimentar novo ciclo.

Em quinto lugar, em todas as fases, principalmente nas três últimas, há a necessidade de «refinar» o conhecimento que se detém, em virtude da volatilidade do SI, pelo que surge a necessidade de dar resposta a questões que possam surgir.

Por fim, os SIN devem garantir a negação da *intelligence*, necessidades e métodos aos SIN adversário durante todo o ciclo.

Importa, então, que os SIN obtenham a vantagem de *intelligence* que permite que o ciclo de decisão se processa mais rapidamente que o do adversário, obrigando-o a reagir a ciclos de decisão mais rápidos que introduzem *inputs* no SI.

4.2. Os atributos da eficácia

Não obstante das dificuldades inerentes à identificação de atributos mensuráveis do produto da *intelligence* importa referir que esse desafio foi, por nós identificado, num autor, Jennifer E.Sims. Para a Doutora Sims a eficácia da *intelligence* depende de quatro funções críticas: a pesquisa – centra-se na pesquisa de informação acerca dos competidores, incluindo a estrutura da competição, a antecipação – que tem o foco na antecipação de novas competições, a transmissão – a comunicação entre decisores e SIN e a degradação dos sistemas adversários – onde se procura a degradação das funções anteriores de forma a garantir uma vantagem competitiva.

Contudo, fruto do entendimento de *intelligence* da Doutora Sims a sua análise não entra em linha de conta com uma das actividades da *intelligence*, a acção coberta, e a, consequente, possibilidade de disrupção do ciclo de decisão adversário. Atributo que nos parece importante, e que sem ele não é possível obter um entendimento holístico da problemática em questão.

Tendo a percepção de que a vantagem de *intelligence* se reflecte na vantagem de decisão, é equacionar que a *intelligence*, sob um ponto de vista holístico, contribui, de forma directa ou indirecta, para que o decisor alcance a vantagem de decisão (conforme figura IV.3). Um Sistema de Informações é mais eficaz se conseguir garantir, aos decisores, a vantagem de decisão em relação ao adversário. Pelo que uma organização deverá direccionar todas as funções que realiza nesse sentido. Parece-nos, então, que a noção de *intelligence* apresentada pelo Prof. Heitor Romana «abre portas» para o conceito de eficácia. Através desta noção, que favorece uma abordagem holística, é possível abranger todas as funções inerentes à necessária redução da incerteza do meio, por um lado, e geradoras de incerteza no processo de decisão adversário, por outro, as duas dimensões da eficácia.

4.2.1. O conhecimento

A primeira dimensão do conceito, a geração de conhecimento, implica todos os elementos necessários para alimentar o processo de decisão e obter a vantagem de decisão. Apoia a decisão ao reduzir a incerteza, permitindo iniciativa na acção. É a produção de *intelligence* de qualidade – oportunidade e relevância[139]. Produz um efeito centrípeto no ciclo de decisão. Incorpora as capacidades críticas: integração, comunicação e antecipação.

4.2.1.1. Integração

É, de acordo com o dicionário de língua Portuguesa a acção de integrar que é "*1 – tornar inteiro; 2 – incluir num todo; incorporar*" (2006: 958). No contexto da eficácia de um SIN poderá ser entendido como a forma sinérgica do sistema operar, seja no quadro da pesquisa, seja no da análise. A integração pode ser mensurável a partir de três factores: o número de subsistemas disponíveis; o alcance da sua cobertura; o grau de sinergia que gera.

O racional subjacente à integração é o de obter *intelligence* de qualidade que, de acordo com Sims (2009: 68), relativamente a um «alvo», varia de acordo com: o número de sistemas disponíveis, o seu acesso ao «alvo» e o grau com que os sistemas são geridos, colectivamente, em apoio aos decisores. Assim, só gestores que tenham conhecimento acerca das vantagens e desvantagens, de cada método, é que poderão optimizar o desempenho dos sensores de pesquisa.

Para além do mais, no atinente à análise e partilha de *intelligence* a necessidade de integração fica patente quando os SIN têm de dar uma resposta célere aos desafios contemporâneos. Para isso, uma das exigências é a de um processo de cooperação robusto entre as agências do SIN, que tutelam os diferentes métodos de pesquisa e, consequentemente, a *intelligence* que deriva da análise das diversas plataformas ou sensores críticos. Permite-se, assim, que haja valor-acrescentado reduzindo o erro inerente à incerteza.

Contudo, atingir este grau de sinergia pode ser difícil quando órgãos diferentes controlam plataformas ou sensores críticos. Nesse sentido, Lowenthal refere que todos os diagramas organizacionais, por muito sofisticados que sejam são enganadores. Reproduzem onde as agências se colocam relativamente às outras, mas não conseguem reproduzir como interagem e quais as relações que têm importância e porquê. "Moreover, personalities do matter. However much people like to think of governments as one of laws and institutions, the personalities and relationships of those filling important positions affect agency working relations*"* (2006: 38). Ficando patente que a integração, elemento gerador de sinergias dos diferentes métodos ou disciplinas da pesquisa e análise está dependente das personalidades que ocupam lugares de decisão nas diferentes agências. A dificuldade de integrar os diversos órgãos de pesquisa e análise da comunidade de *intelligence*, a que Lowenthal

[139] Adequado – às necessidades do decisor; claro – quanto à forma de transmissão; distinto – separar o conhecido do desconhecido.

faz referência é verdade para Estados, como os EUA, onde a comunidade de *intelligence* e o sistema coincidem. Nesse sentido, ser-nos-á possível inferir que, em Estados em que a comunidade de *intelligence* não coincide com a organização do SIN, essa dificuldade será maior e a capacidade de integração da pesquisa e análise são muito menores, ficando, nessa situação, a integração dependente de contactos informais.

4.2.1.2. Comunicação

A Comunicação é, neste contexto, assumida como o estabelecimento de relações e transmissão de informação entre indivíduos ou grupos. É uma característica que afecta, directamente, a *intelligence* de qualidade.

Requer, de acordo com Sims (2009: 77), a confiança entre os SIN e decisores. Para aquela autora esta característica, ainda que seja de difícil mensuração, mede a proximidade dos SIN aos decisores e a profundidade das suas comunicações, antes da decisão. O racional é o de que os SIN serão uma extensão dos ouvidos e olhos dos decisores. No entanto, a proximidade não pode, nem deve diminuir a confiança das duas partes. A comunicação é medida através do grau de confiança entre decisores e SIN.

O afastamento entre decisores e SIN surge quando o decisor deixar de acreditar no trabalho do SIN. Para Gazit (1989: 264) esta situação prende-se com a aceitação. Para aquele autor aceitação significa que a *intelligence* é aceite e percebida cognitivamente, para além de que é entregue ao seu utilizador em tempo. A aceitação cognitiva implica, para Gazit, que o conhecimento é assimilado e todos os aspectos da estimativa de *intelligence* são percebidos. Para isso deverão existir procedimentos de rotina entre os dois intervenientes: discussão e deliberação. A relação de confiança entre SIN e decisores advém desta relação e sem ela a confiança, mútua, é muito difícil de alcançar. A segunda, implica que a *intelligence* deverá se entregue ao utilizador em tempo, de modo a ser utilizável. Nesse sentido, numa lógica de confiança, para aquele autor, a entrega em tempo implica a possibilidade do decisor testar o conhecimento antes de o utilizar. Gazit (1989: 270) acrescenta que, para esse efeito, o decisor poderá, à semelhança de Estados como Israel, possuir grupos de analistas cuja tarefa é testar o conhecimento. A questão que se coloca prende-se com a sensibilidade e secretismo inerente a este tipo de informação. Israel resolveu esse problema ao incorporar académicos proeminentes no corpo de *intelligence* nas forças reservistas da IDF. Para além do mais, para aquele autor, a «forma» como o conhecimento é entregue ao decisor é outro ponto que pode ter impacto na comunicação (Gazit, 1989: 271). Será então importante que os SIN disseminam o conhecimento na «forma» certa para garantir a percepção da comunicação, já que os decisores "are busy people, so used to persuing or skimming over a greta quantity of written material that they easily become accustomed to a routine of written reports only*"* (Gazit, 1989: 271). Para isso, Gazit (1989: 272) refere que reuniões regulares facilitam, não só, a empatia entre SIN e decisores como permitem que sejam clarificadas questões relativamente à *intelligence*, que transcendam os relatórios, e a comunicação de quesitos aos SIN, o que facilita a

alocação, mais célere, de meios o que facilita a antecipação.

Para além do mais, esta relação não depende exclusivamente da disseminação. A montante encontra-se a relação entre decisores e SIN materializada na orientação do esforço de pesquisa[140] e, após a disseminação, o *feedback*, tão necessário para que se possam corrigir diferenças entre as necessidades e o produto.

O importante será manter uma relação de confiança nem demasiado próxima nem demasiado afastada. Para que tal seja possível, deverá haver um grau de independência dos SIN, relativamente aos decisores. O equilíbrio deverá ser atingido através da confiança e proximidade em contraponto ao afastamento e controlo.

Todavia, internamente também surgem situações que podem interferir na confiança, mormente, pela falta de comunicação entre a pesquisa e a análise. O facto de estas operarem, amiúde, independentemente – os relatórios da pesquisa são do conhecimento dos decisores, por vezes, primeiro que de analistas. Estes *stovepipes* podem ser a causa de incongruências entre relatórios da pesquisa e da análise, o que naturalmente pode causar a falta de confiança entre SIN e decisores e, consequentemente, da comunicação.

Idealmente os SIN avaliam e alertam acerca de perigos conhecidos, mas também de possíveis desenvolvimentos para os quais os decisores deverão estar preparados, tais como: novos adversários, que podem obstar à consecução dos seus objectivos, ou eventos que podem sugerir que as suas políticas poderão não ter sucesso. Nesse sentido, os SIN deverão garantir que as capacidades de gerar conhecimento são independentes das preferências políticas, de forma a evitar a politização da *intelligence*, *top down* ou *bottom up*, o que vai, necessariamente, desvirtuar o produto dos SIN.

Para Jennifer Sims os decisores que forem apoiados por um SIN que se faça ouvir, terão mecanismos para testar e escrutinar a *intelligence* mas não terão a capacidade de controlá-lo completamente, esse controlo será efectuado através dos sistemas de fiscalização executivo e legislativo (2009: 82).

4.2.1.3. Antecipação

É a razão de ser dos SIN. Se um SIN não conseguir antecipar possíveis conflitos, prever ameaças relacionadas e oportunidades e identificar novos decisores – próprios e adversários – perde o seu sentido de missão e torna-se irrelevante (Sims, 2009: 71), pelo que o seu impacto no ciclo de decisão é directo.

É a disseminação em tempo, ao decisor apropriado, que objectiva o cumprimento do alerta precoce. Para esse efeito, também a orientação do esforço de pesquisa tem capital importância. O incremento de celeridade introduzido no processo gerador de conhecimento, pelo conhecimento de objectivos e

[140] Que permite que os órgãos de pesquisa sejam direccionados para missões que concorram directamente para as necessidades dos decisores, através do conhecimento dos objectivos e intenções dos decisores.

intenções de decisores permite a criação de linhas de limite temporal, ficando-se, assim, com a noção da oportunidade que determinado produto carece. Para além disso, o produto produz influência na antecipação. Os decisores têm, por norma, as suas preocupações centradas no imediato, pelo que a *intelligence* corrente tem a primazia relativamente à estimativa ou aos indicadores e alertas. Esta situação que leva um SIN se centre em demasia na *intelligence* corrente poderá relegar para segundo a estimativa e os indicadores e alertas. Ao colocar o esforço da análise num determinado tipo de produto, implica que se investe em competências, de analistas, compatíveis com essa opção. Assim, os produtos que permitem a antecipação – estimativas e indicadores e avisos – ficam limitados, bem como a capacidade de antecipação.

Jennifer Sims, ao debater as questões da antecipação e da identificação de surpresa, aponta como principais lacunas: (*i*) não conhecer o adversário – falta de visão estratégica; (*ii*) saber que é o adversário mas desconhecer a ameaça que coloca – falta de visão táctica; (*iii*) conhecer o adversário, conhecer a ameaça que coloca, mas desconhecer que tem necessidade dessa informação – falta de conhecimento próprio; (*iv*) conhecer os anteriores elementos mas não disseminar em tempo a informação ao decisor que dela necessita (Sims, 2009: 73). De qualquer forma identificar, antecipadamente, os decisores que necessitam da *intelligence* é crucial para a eficácia dos SIN.

A identificação de novos utilizadores de *intelligence* pode ser uma das responsabilidades dos decisores, contudo, é também uma tarefa das estruturas de *intelligence,* o que requer uma forte cooperação entre SIN e decisores. Nesse sentido, as sociedades organizadas burocraticamente oferecem vantagens sobre as sociedades tribais ou outras. Assentes na «divisão de trabalho», as sociedades organizadas burocraticamente, permitem a identificação de novos decisores através das suas funções. Sendo, igualmente, verdade para adversários cuja organização assente numa burocracia.

Contudo, os esforços dos SIN podem encontrar obstáculos próprios da burocracia. Sendo a *intelligence* um recurso limitado, os decisores com acesso àquele recurso poderão resistir relativamente à perda da primazia do acesso ou permitir que outros compitam pelo apoio de *intelligence* (Sims, 2009: 73). Assim, a capacidade de antecipação de um sistema, para além da disseminação do conhecimento, ao decisor adequado, em tempo útil depende da habilidade dos SIN em se distanciar dos utilizadores que, normalmente apoia e seleccionar de forma eficaz aqueles que têm necessidade de conhecer.

4.2.2. A negação

A negação é a segunda dimensão do conceito de eficácia. Procura induzir o adversário em erro ou disromper o seu ciclo de decisão, pelo que, terá como efeitos o incremento da amplitude do seu ciclo de decisão, obrigando-o a reagir. Pretende-se que produza um efeito centrífugo no ciclo de decisão do adversário. Incorpora as capacidades críticas de degradação dos sistemas adversários e a disrupção do ciclo de decisão adversário. Tem como racional a acção centrífuga no ciclo de decisão adversário.

4.2.2.1. Degradação do sistema adversário

A degradação do sistema adversário é a capacidade de criar fraquezas num SIN adversário e transformá-las em ganhos. Degradar o sistema adversário pode torna-lo mais vulnerável à decepção, o que vai, com certeza, interferir na sua capacidade de antecipação. O racional é o de interferir com as capacidades críticas da dimensão geradora de conhecimento, do adversário. O seu «alvo» são os SIN adversários, entrando, por isso, no racional da CI.

Assim, como foi anteriormente descrito, a função *counterintelligence* assume duas dimensões: a dimensão passiva e a dimensão activa.

Na primeira, o racional é o de proteger as capacidades, intenções e actividades do próprio SIN. Se tal desiderato for atingido, recorrendo aos sistemas de classificação da informação e às medidas de segurança, garante-se que o adversário terá dificuldade em gerar conhecimento necessário à decisão, já que os seus sistemas de pesquisa encontram uma «barreira» que os impede de percepcionar o ambiente, degrada-se a capacidade de integração. Para além do mais, ao limitar a sua capacidade de mitigar a incerteza do meio incrementa-se o seu ciclo de decisão, garantindo que reage aos *inputs* à medida que eles se manifestam. Atinge, por isso, o estado de «cegueira» necessário para induzi-lo a uma decisão desestruturada. Obtém-se a vantagem da decisão, através da degradação da antecipação.

As medidas activas de *counterintelligence*, a contra-espionagem, a CI multidisciplinar e a decepção e contra-decepção, procuram, por um lado, criar a falsa percepção do ambiente externo e a consequente mitigação da incerteza pela introdução de dados falsos, nos seus SIN, que o induzam em erro, através da decepção. Nesse sentido, a lógica é a de criar a falsa sensação de que o seu ciclo terá uma amplitude suficientemente pequena que lhe permitirá agir, em vantagem. Porém, essa acção irá ao encontro dos interesses da outra parte, retirando-lhe, na base, a vantagem de decisão. A lógica destas acções, para além da inserção da incerteza no ciclo de decisão adversário é o de descredibilizar o SIN adversário, junto dos decisores a quem tem de apoiar. Afecta-se a comunicação.

De mais a mais, por via da contra-espionagem e da CI multidisciplinar, é permissível ter acesso às capacidades, técnicas e métodos do SIN adversário. Tais acções facilitarão a obtenção do conhecimento necessário para a identificação de vulnerabilidades próprias e, assim, protegê-las das investidas dos SIN adversários e limitar a capacidade de degradação dos sistemas do adversário.

4.2.2.2. Disrupção da decisão adversária

A disrupção da decisão adversária tem como «alvo», directo, o ciclo de decisão adversário, ao invés dos seus SIN. O racional subjacente a este factor é o de destruir, ainda que momentaneamente, o ciclo adversário. Seja pelo incremento de *inputs* que recebe, *information overload*, e que não tem capacidade de processar, seja pela destruição do ciclo através da eliminação do decisor.

Latu sensu coincide com a função acção coberta da *intelligence*. A acção coberta, como anteriormente descrito, possui quatro categorias: a propaganda; a acção coberta política; a acção coberta económica; e a acção paramilitar. É certo que, como já foi anteriormente debatido, a decisão

por esta opção não é da lavra dos SIN. A capacidade de decisão do emprego desta função de disrupção é sempre do decisor, político. Contudo, são actividades desenvolvidas pelos SIN aquelas que permitem ganhar a vantagem de decisão sobre o adversário, pela disrupção total ou parcial do seu ciclo de decisão.

Nas três primeiras, o enfoque deve ser dado ao incremento de *inputs* colocados ao decisor adversário. O racional é o de causar dificuldade de leitura do ambiente,aos decisores, em virtude de um aumento, significativo, da complexidade dos condicionalismos[141] da sua acção, na condução do processo de decisão em política externa. Procura-se atingir este desiderato através do aumento do *stress*[142] dos decisores adversários de modo a fragmentar o seu ciclo de decisão. Para tal exerce-se influência na opinião pública, através da propaganda, da acção coberta política e da acção coberta económica, de modo a pressionar as elites decisoras que, segundo Bessa, são "…predominantemente burguesas desterritorializadas, que estão muito interessadas na sua própria manutenção à cabeça do Estado e que dependem da sensibilidade do eleitorado*"* (2001: 126) .

As actividades paramilitares, através de acções como por exemplo de raptos ou *Target killing*, têm como racional a eliminação de decisores ou entidades consideradas críticas para o desenvolvimento de estratégias ou políticas do adversário. O Ciclo de decisão não incrementa ou diminui, desaparece, simplesmente, ainda que momentaneamente. A título de exemplo referimo-nos às actividades de rapto ou *Target killing* desenvolvidas por Israel, através do seu SIN, contra elementos proeminentes das organizações tidas como inimigas ou da campanha desenvolvida por aquele Estado contra o programa de desenvolvimento de tecnologia nuclear iraniano, onde através do seu SIN, aquele Estado, eliminou vários cientistas iranianos com um papel de relevo no referido programa (Fratini, 2011). A lógica é atrasar o programa de desenvolvimento nuclear iraniano de forma a limitar a liberdade de acção, daquele Estado, na arena internacional, de forma a retirar-lhe vantagem na decisão.

4.2.3. A vantagem de intelligence

Para se alcançar a vantagem de decisão há duas formas possíveis: obter melhor informação que o adversário e, assim, diminuir a amplitude do ciclo de decisão ou degradar a dimensão geradora de conhecimento adversário, ao mesmo tempo que protege a informação própria, de forma a incrementar o ciclo de decisão adversário (conforme figura IV.3).

[141] Bessa identifica como condicionalismos os parâmetros estritamente pessoais e de ordem psicológica; o tempo – o prazo da decisão; o valor e capacidade dos decisores; a pressão do eleitorado (2001: 124-126).

[142] Neste contexto o *Stress* pode ser entendido na perspectiva de Renshon e Renshon como "…as na excess of demands over capacities. It can be introduced by following variables, either alone or in combination: threat to important values (…) anxiety, or severe time pressure (…) And in crisis, the factors may be exacerbated even further and contribute to poor decision process*"* (2008: 512-13).

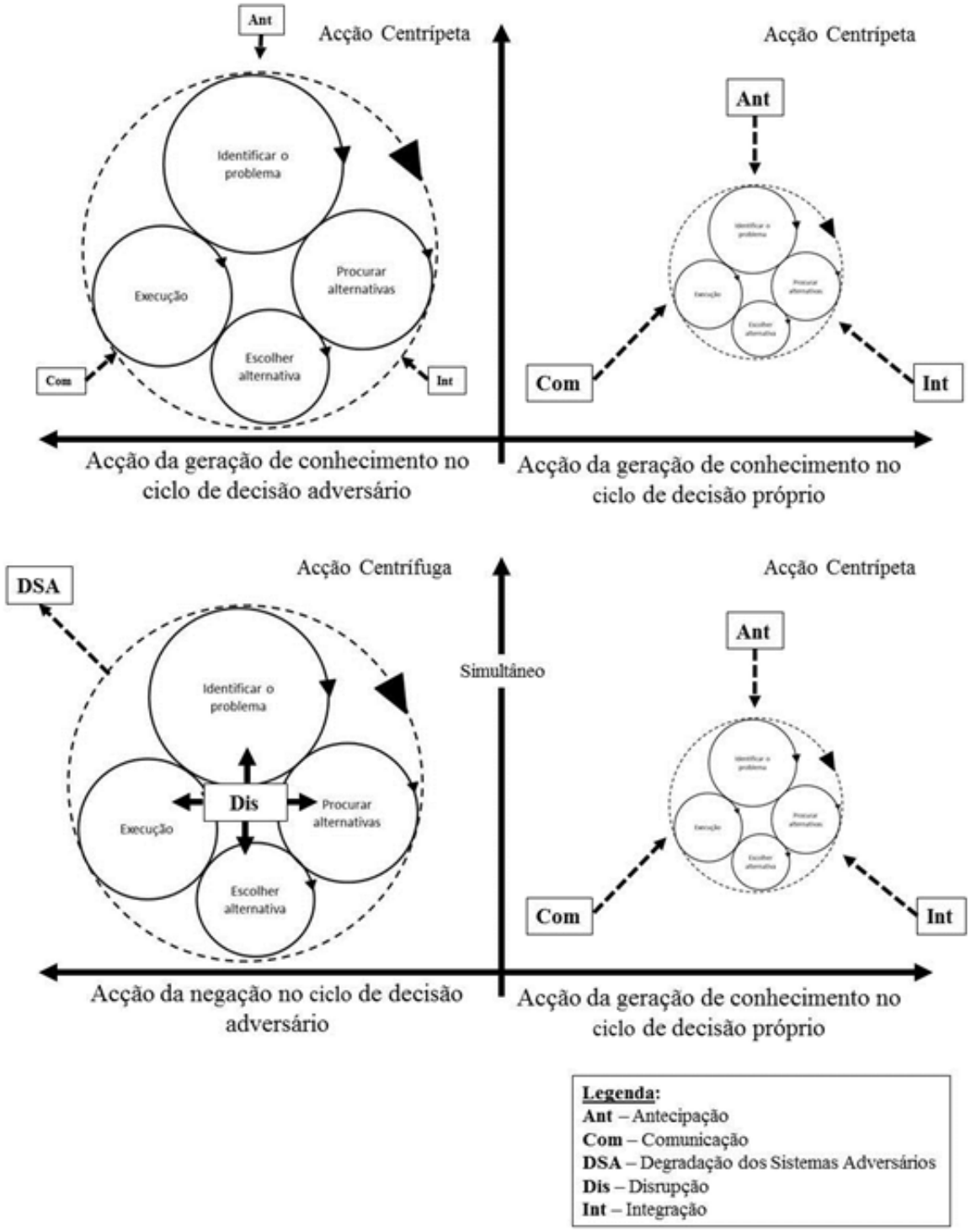

Figura IV.3 – Impacto da vantagem de *intelligence* no ciclo de decisão

Nesse sentido, as falhas de *intelligence* não devem ser entendidas como inexactidão mas como perda da vantagem de *intelligence*, relativamente ao adversário. Da mesma forma, os sucessos poderão ter menos que ver com a obtenção de *intelligence* «perfeita» – que para Robert Jervis, citado por Sims (2009a: 63), significa a situação ideal na qual há um completo conhecimento acerca da situação em

termos de alerta precoce, inclui a previsão de decisões relevantes tomadas pelo adversário – do que com a consecução e manutenção da superioridade perante o adversário. Assim, ainda que a *intelligence* possa não obter conhecimento perfeito poderá ganhar vantagem sobre o adversário, desde que garanta que o adversário toma decisões piores e, consequentemente, mais erros de decisão ao longo do tempo. Pelo que um SIN será tão eficaz quanto maior vantagem de decisão oferecer aos utilizadores da sua *intelligence.*

Olhando para as suas capacidades críticas o racional é o de procurar maximizar as capacidades próprias, em relação às do adversário, procurando transformar os seus pontos fortes em pontos fracos e, consequentemente, em vulnerabilidades que possam ser exploradas. Assim, se um SIN adversário for forte na característica de degradação dos sistemas adversários pode-se incrementar a integração, através da partilha de *intelligence* e incrementar a sinergia dos sistemas de pesquisa de modo a evitar as acções de decepção. Para além do mais, se as medidas passivas de CI forem fracas, pode-se incrementar as acções de decepção.

Se a sua capacidade de integração for forte, pode-se maximizar a degradação dos sistemas adversários pela acção de operações de decepção conjugadas com acções de segurança passiva, procurando, por um lado a «cegueira» do adversário e, por outro, induzi-lo em erro. Estas acções, para além de degradarem a capacidade de integração interferem, de forma substancial, nas suas capacidades de comunicação – ao procurar degradar a confiança entre decisores e SIN – e, através das operações de decepção, degradar a capacidade de antecipação.

Importa, ainda, fazer referência, a título de exemplo à capacidade crítica disrupção. Nesse sentido, se o adversário possuir, como ponto forte essa capacidade, poder-se-á incrementar a capacidade de integração. Com a maximização da integração poder-se-á ter acesso a um conjunto de informações que poderão ser usadas através da propaganda ou outro método de disrupção, ou de CI, que transformem aquele ponto forte do adversário em vulnerabilidade, seja ao nível interno, seja ao nível internacional.

Partilhando o racional de Jennifer E. Sims (2009a: 69), analisar as capacidades dos SIN implica desagregar e comparar as suas capacidades à luz das dimensões, atrás citadas, e consequentemente, das características que as compõem. A lógica implícita é a de que actores que sejam, relativamente, mais fracos em qualquer característica deverão compensar desenvolvendo forças relativas noutras, de modo a minimizar o impacto e garantir a vantagem relativa de *intelligence.* Na incapacidade de comparar dever-se-á ter em linha de conta o racional da maximização de todas as dimensões da eficácia de um SIN.

4.3. Flexibilidade organizacional

É o grau de adaptabilidade do SIN, tendo em conta as necessidades dos executivos e o ambiente externo. É, por isso, um facilitador da eficácia.

É certo que o Estado é uma organização burocrática, por natureza, e os SIN, como parte integrante do Estado, também o são. A burocratização assume especial importância na organização dos SIN onde

a «divisão de trabalho» se prende com questões de compartimentação relacionados com a segurança dos processos, actividades e produtos. Esta rigidez burocrática introduz obstáculos significativos à dimensão geradora de conhecimento, em todos os seus indicadores.

O século XXI, fruto das alterações significativas do ambiente em que os SIN operam veio trazer modificações relevantes na forma de entender as suas necessidades e a forma de operar. A alteração dos «alvos» e a forma de encarar a análise (de *puzzle* para complexidade) veio demonstrar a dificuldade de adaptação aos novos desafios que requerem respostas rápidas, conduzindo o paradigma do *need to know* à necessidade de adaptação ao paradigma do *need to share*. Ficando patente a necessidade do SIN se «moldar» às necessidades, adaptar-se. Nesse sentido, a adaptabilidade prende-se com o grau de adequabilidade organizacional de um SIN às necessidades impostas pelo meio, de forma preemptiva.

Se um Estado não tiver a capacidade de se adequar ao meio externo, corre o perigo das suas estruturas não conseguirem obter a eficácia necessária. Por exemplo, a dificuldade de integração, patente na falta de cooperação e partilha de *intelligence* interagências, é tido como uma das primeiras razões pelas quais não foi possível antecipar os eventos de 11 de Setembro nos EUA, para além do mais, a se a estrutura não tiver capacidade de se adaptar de forma célere, a eficiência é dificultada e, ao invés de se obterem sinergias entre as diversas agências que compõem o SIN, cria-se a duplicação de esforços. Essa duplicação, tende a dificultar a comunicação do SIN com os decisores, pelo incremento de informação contraditória que dificultará a oportunidade e relevância, condições necessárias para a criação de confiança entre decisores e SIN. Para além do mais, a capacidade de adaptabilidade do SIN ao meio, está directamente relacionado com as necessidades dos decisores, em tempo, a antecipação. Afinal, o racional subjacente à existência dos SIN é o apoio que prestam à decisão das elites executivas de um Estado, pelo que a organização dos SIN reflecte as necessidades de *intelligence* dos decisores. Um SIN, cuja capacidade de adaptação ao meio seja alta pode indiciar que as decisões são suportadas pelo conhecimento gerado pelos SIN.

É certo que à primeira vista este desiderato representa uma impossibilidade, em virtude do cariz rígido da burocracia, contudo, de acordo com Chiavenato (2004: 277) nem todas as burocracias são iguais, variando de acordo com seis factores: (*i*) a divisão do trabalho – da especialização à generalização; (*ii*) a hierarquia – da autoridade à ausência da mesma; (*iii*) as regras e regulamentos – da ordem e disciplina à liberdade excessiva; (*iv*) a formalização da comunicação – do excesso de formalismo à ausência de documentação; (*v*) a impessoalidade – da ênfase no cargo à ênfase nas pessoas; (*vi*) a selecção e promoção – do excesso de exigências ao apadrinhamento. Nesse sentido o grau de adaptabilidade de um SIN passa por agilizar os factores de que depende uma organização burocrática.

Por exemplo, flexibilizar a divisão de trabalho não implica que se prescinda da especialização, pode passar pela criação de grupos de discussão – e.g. *think tanks* – ou *fusion centers* os quais permitem a reunião de vários especialistas, garante-se, assim, a sinergia dos diversos elementos em

detrimento da estanquicidade colocada na especialização das agências. Para além do mais, a possibilidade de criação de estruturas, daquele tipo, permanentes ou temporárias, não obriga a uma estrutura organizacional hierarquizada podendo assumir uma estrutura matricial, tal como Treverton aconselha. Esta oferece a necessária adaptabilidade e integração que garante uma maior partilha e cooperação do SIN, mitigando, desse modo, o efeito inflexível da burocracia. Outra forma de flexibilizar a burocracia é através de maior liberdade de acção aos seus membros. Ainda que possa ser um contra censo no que respeita às necessidades de segurança, dos SIN, esta questão pode ser obviada através de um sistema de fiscalização externo mais vincado e presente, de forma a escrutinar as acções tomadas por SIN e decisores. Garante-se, assim, que não há quebras de segurança acerca de conhecimento, processos e métodos, por um lado, e que não há abusos de poder ou de autoridade, por parte dos SIN ou decisores, por outro.

4.4. A fiscalização externa dos SIN

O debate acerca da eficácia dos SIN não ficaria completo, em nosso entendimento, se não fosse abordada a questão da fiscalização externa dos SIN. A sua importância é induzida através das dimensões de conhecimento e da necessária flexibilidade, através da adaptabilidade. A fiscalização permite o distanciamento dos SIN, relativamente aos decisores, evitando a sua instrumentalização. Depois, facilita a flexibilidade através da liberdade de acção dos elementos das estruturas burocráticas, assegurando que os propósitos para os quais existem são respeitados, já que garante o "controlo das actividades operacionais (cobertas) e a certificação de que estas não violam princípios, direitos, liberdades e garantias constitucionalmente reconhecidos sem que, para o efeito, estejam mandatados politicamente e cobertos por lei" (Esteves, 2004: 441). Deve ser, por isso, entendido com um facilitador da eficácia e da transparência nos Estados democráticos.

Para que tal seja possível a fiscalização dos SIN deve ser feito em três níveis: o nível interno, nível executivo e o nível externo.

Ao primeiro nível corresponde a direcção do SIN e ao nível do executivo os órgãos dependentes do governo. O primeiro através do seu director, de acordo com directivas ministeriais, através de estatutos ou outra legislação emanada pelo parlamento nacional. O estatuto reflecte as preferências políticas. Ao nível do controlo governamental o padrão é o controlo extra-organização pela criação de estruturas de direcção, orientação e coordenação, sendo mais complexas, quanto maior é o grau de valorização política dos SIN (Esteves, 2004: 443-444).

Apesar do primeiro nível de fiscalização ser efectuado ao nível interno esta deve ser reforçada pelo nível executivo e pelo nível externo – comissões parlamentares e, quando apropriado, pelo poder judicial. Para além do mais, e opinião pública e os media também podem providenciar o escrutínio, ainda que esporadicamente (Gill e Phythian, 2006: 156).

A necessidade da fiscalização externa prende-se, essencialmente, com o facto dos mecanismos internos apresentarem um carácter, algo problemático (Esteves, 2004: 442). Primeiro porque o segredo

que enforma as actividades de *intelligence* tornar-se o foco do exercício do controlo ou fiscalização de elementos, potencialmente perturbadores do SIN. Depois, o facto dos SIN estarem dotados de alguma autoridade discricionária, especialmente no que concerne às actividades que desenvolvem, levantam questões acerca do controlo hierárquico e da autoridade, especialmente em Estados democráticos. Para além do mais, de acordo com aquele autor, existe uma política de mistificação dos SIN que espelha a renitência do poder político, em democracia, intervir nas actividades daqueles órgãos. Os SIN, por seu turno, procuram acentuar o desiderato de não intromissão.

O primeiro mecanismo do nível externo é o controlo parlamentar. O parlamento detém a legitimação política conferida pelo escrutínio popular, possui um "papel determinante como barómetro dos níveis de responsabilização política serviços de informações*"* (Esteves, 2004: 444). Para aquele autor a eficácia do escrutínio parlamentar depende do funcionamento do sistema, do carácter vinculativo da comissão em relação ao governo, da amplitude do acesso a documentos, do grau de credenciação, da sua especialização ou da capacidade de iniciativa da comissão. Apesar destes factores, para Esteves, este nível não tem capacidade de influência, não dispondo de meios de fiscalização directa. É possível que a razão para a ineficácia deste nível de fiscalização esteja relacionada com questões que se prendem com as agendas políticas. Para Jennifer E. Sims (2009: 80) a *intelligence* de qualidade não é neutral, o que dificulta o controlo parlamentar nas democracias, onde a oposição detém um papel de fiscalização. Tão crucial como a fiscalização é manter a qualidade de um SIN – em grande medida porque incrementa a confiança entre as elites eleitas, os sistemas de *intelligence* e o eleitorado – a fiscalização da execução envolve-se numa expectativa de apoio político à agenda legislativa. Quando um SIN se empenha com diferentes centros de poder, com preferências estratégicas diferentes, e procura servir cada um deles corre um risco alto de perder a eficácia. Isto porque a lealdade do SIN à estratégia do executivo pode tornar-se suspeita e pode levar à quebra de confiança, factor que determinante para a comunicação.

O segundo mecanismo de fiscalização externa, o controlo judicial, tem o enfoque, com poder vinculativo, "ao nível da conformidade legal das operações (…) e da gestão dos dados na sua posse*"* (Esteves, 2004: 444). Contrariamente ao papel desempenhado pelo controlo parlamentar, a participação do poder judicial, através de magistrados, constitui "um elemento da estabilidade política no sistema*"* (Esteves, 2004: 445), ainda que, segundo aquele autor, a sua influência na responsabilização e moralização dos SIN seja reduzida.

Por fim, a opinião pública que espelha as manifestações de cidadania onde os vários sectores organizados da sociedade – partidos políticos e NGO, por exemplo – e os indivíduos expõem e trazem à discussão pública as actividades, dos SIN e do executivo, consideradas abusivas ou violadoras dos direitos, liberdades e garantias dos cidadãos, ainda que para esse efeito, acedam a informação em quantidade muito limitada. Para Caparini (2007: 12) essa informação pode ser voluntariamente libertada de forma sistemática ou episódica através de esquemas legais de desclassificação de informação ou através de fugas de informação dos SIN. Sendo o racional da utilização por parte de

cidadãos ou movimentos de cidadania a influência das políticas do executivo.

Os *media* constituem-se como o tecido que liga indivíduos, grupos de cidadania e governos, tendo por isso um papel fulcral nas alterações da opinião pública e nas preferências políticas. Num Estado democrático os *media* desempenham um papel de «observação» dos governos, que opera independentemente do controlo político, através da liberdade de imprensa. Assim, tendo como objectivo primário de informar a opinião pública, consegue garantir que esta tem acesso às acções, decisões e abusos de poder por parte do executivo. Procura garantir a transparência do sistema.

CONCLUSÕES

Com a presente dissertação de mestrado pretendemos investigar quais os elementos determinantes para que um SIN possa ser considerado eficaz. O objectivo da investigação proposta pretendia averiguar a inserção da *intelligence* no ciclo de decisão em política externa sob a perspectiva holística, proposta por Sherman Kent: a *intelligence* enquanto organização, conhecimento e actividade. Delimitámos a investigação, no que concerne ao vector geográfico, aos SIN com origem em Estados assumidos como democracias ocidentais, no atinente ao âmbito de actuação, à política externa e, finalmente, no que diz respeito ao vector temporal, ao período pós – 11 de Setembro, data a partir da qual o «mundo» despertou para novos desafios no quadro da segurança externa. Pelo que, as conclusões desta dissertação não podem estender-se para além da referida delimitação, sem que, para tal, se desenvolvam os estudos apropriados.

A perspectiva, sob a qual pretendemos estudar a problemática proposta, foi assente num entendimento de desequilíbrio do adversário pela criação de vulnerabilidades em função da deterioração do seu ciclo de decisão, a *Auftragstaktik*. E, para isso, é de suprema importância o emprego da *inttelligence.* Este entendimento coincide, na essência, com o que Sun Tzu preconizava, cerca de 500 a.C. na longínqua China, "…a excelência suprema consiste em quebrar a resistência do inimigo sem combater" (2006: 77).

Para abordar a temática proposta "Sistemas de Informações Nacionais. Contributos para a percepção da eficácia" definiu-se como fio condutor a seguinte questão central: *Como se pode medir a eficácia de um SIN, no âmbito da política externa de um Estado?*

Com esta pesquisa procuramos, inicialmente, encontrar a compreensão do conceito de *intelligence* bem como o entendimento do que é um sistema de informações nacional. Foi permitido identificar, que a *intelligence* é uma actividade desempenhada por Estados de forma a facilitar a consecução dos seus fins últimos e que os SIN são organizações permanentes designadas para apoiar esse desiderato no quadro da redução da incerteza. Para além do mais, as funções que os SIN desempenham no Estado podem ser de garantir a experiência de longo prazo aos decisores, o apoio no processo de decisão e a garantia do segredo da informação, necessidades e métodos. Para além do mais, foi ainda possível, no atinente à organização daquelas estruturas, perceber que reflecte as necessidades e prioridades do governo, quanto à *intelligence*.

De seguida, tendo o enfoque colocado no conhecimento e no processo gerador daquele recurso identificámos que o ciclo de produção de informações é o processo pelo qual é possivel produzir o conhecimento necessário para alimentar o processo de decisão, ainda que apresente descrepâncias com a realidade, as quais são passíveis de produzir um impacto negativo na pertinência e oportunidade, por via das deficiências de comunicação. Primeiro, a falta de orientação do esforço de pes quisa, necessário para dar início ao processo, na maior parte das vezes não é objectivada, o que pode ter impacto na oportunidade e relevância do conhecimento. Em segundo lugar, as dificuldades de comunicação entre pesquisa e análise que operam, muitas vezes, em paralelo. Em terceiro lugar, a falta

de *feedback*, na disseminação do produto, não permite que os SIN tenham conhecimento das necessidades dos decisores, de forma a poderem melhorar os processos de geração de conhecimento. Nesse sentido, a qualidade do conhecimento pode ficar aquém das necessidades dos decisores o que poderá incrementar a falta de confiança entre decisores e SIN. Identificámos, ainda, que para que o conhecimento possa ter qualidade terá de possuir as características de oportunidade e relevância: (*i*) adequado; (*ii*) claro; (*iii*) distinto.

Posteriormente, centrámo-nos nas funções da *inteligence*, a terceira componente da abordagem holística, proposta por Sherman Kent. Aqui verificámos que, no tocante à função pesquisa, se salienta a necessidade de integração dos diferentes métodos de pesquisa de forma a garantir que, ao colmatar os pontos fracos de cada um deles, se obtém a sinergia necessária da pesquisa. Da função análise, ressalvamos a necessária integraçao, através da cooperação interagência, a partilha de *intelligence.* Da função *couterintelligence* sobressai a necessidade de protecção das capacidades de *intelligence*, para além das intenções, métodos e conhecimento, através das medidas passivas e induzir o adversário em erro, através das medidas activas, para além de, identificar as vulnerabilidades do próprio sistema de modo a melhor protegê-lo. A função acção coberta opera numa lógica de destruição do ciclo de decisão adversário. O facto desta função ser direccionada conta os decisores adversários implica que o ónus da decisão, de emprego da acção coberta, ser do decisor.

Por fim, procurámos, a partir do ciclo de decisão em política externa, perceber qual a influência que a *intelligence* produz e quais os factores da eficácia de um SIN. No atinente ao ciclo de decisão foi possível identificar que, independentemente do processo de decisão em política externa, este desenvolve-se de acordo com um ciclo de quatro elementos: (*i*) identificar o problema; (*ii*) procurar alternativas; (*iii*) escolher alternativas; (*iv*) execução. Para além dos mais, a *intelligence* tem uma internveniência em todo o ciclo. Para isso possui cinco capacidades críticas agrupadas numa lógica de geração de conhecimento – através da integração, comunicação e antecipação – e, concorrentemente, num racional de negação do conhecimento – degradação dos sistemas adversários e de disrupção da decisão adversária –que podem garantir a vantagem de decisão. Esta vantagem consubstancia-se através da maximização das capacidades críticas em relação ao adversário de forma a infuenciar um ciclo de decisão, com uma amplitude temporal, menor que a do adversário, de forma a obrigá-lo a reagir, preferencialmente, desequilibrado. Caso não seja possível comparar as capacidades críticas, um SIN, para garantir a eficácia, terá de maximizar todas as suas capacidades críticas. Contudo, a incapacidade de adaptação, organizacional, preemptiva às necessidades impostas pelo meio pode ser um constrangimento à eficácia de um SIN. Contudo, a flexibilização da burocracia é possivel, desde que se garanta a fiscalização externa.

Assim, procurando dar resposta à questão que serviu de fio condutor para a presente dissertação, o nosso argumento é de que a eficácia de um SIN pode ser medida através da maximização relativa das capacidades críticas que integram as dimensões geração de conhecimento e negação, de forma obter a vantagem de decisão.

Para dar suporte ao nosso argumento encontrámos quatro razões. A primeira é que a decisão em política externa é tomada tendo em conta um ciclo composto por quatro fases: (i) identificar o problema; (ii) procurar alternativas; (iii) escolher alternativas; (iv) execução.

A segunda é que a vantagem de decisão é alcançada, por via da vantagem de *intelligence,* quando o ciclo de decisão adverário tem uma amplitude superior, obrigando-o a reagir

A terceira é que as características que enquadram a dimensão geradora de conhecimento permitem diminuir a amplitude do ciclo de decisão e as características que são delimitadas pela dimensão negação induzem o adversário num ciclo de decisão mais amplo ou através da disrupção, na destruição do ciclo através do incremento de pressão, causadora de *stress* nos decisores adversários, ou na eliminação do decisor.

A quarta implica que para se obter a vantagem de *intelligence* terá de se incrementar a amplitude do ciclo de decisão adversário através da maximização das características necessárias para tornar os seus pontos fortes em vulnerabilidades.

Olhando para o passado é frequente afirmar-se que D. João II desenvolveu uma política de segredo que apoiou a projeção de Portugal para o patamar de potência internacional. Contudo, D. João II foi mais longe, criou um «sistema» que lhe permitiu obter a vantagem de *intelligence* e, consequentemente, da decisão.

É certo que o «sistema» que apoiava o «Príncipe perfeito» era uma estrutura *ad hoc*, bastante longe dos SIN actuais. Não obstante criou uma estrutura que lhe permitiu obter a vantagem de *intelligence.* Para isso, o «Príncipe Perfeito», cuidou uma "…política de segredo, de recolha de informações e de deformação dessas mesmas informações…" (Cardoso, 2004: 32) que permitiu negociar com um adversário desequilibrado e, assim, obter a vantagem na mesa de negociações, em Tordesilhas. Nesse sentido, permitiu a Portugal a primazia das rotas comerciais da Índia e a salvaguarda de um território que, posteriormente, veio a mostrar-se vital no contexto imperial português, o Brasil.

Pelo carácter mensurável, ainda que seja qualitativo, e relativo que esta abordagem atribui à *intelligence* presumimos que esta dissertação abre caminhos para estudar a *intelligence* enquanto um poder funcional[143] do Estado.

Para alcançar o desiderato da eficiência, sem incorrer no perigo de macular o produto, e consequentemente, a eficácia de um SIN importa, então, ter presente as características: integração; comunicação; antecipação; degradação dos sistemas adversários; e a disrupção da decisão adversária. Sabendo de que forma se obtém a vantagem de *intelligence* consegue-se reestruturar e reformular um SIN sem que a qualidade da *intelligence* possa ser afectada.

[143] Para Adriano Moreira "*Trata-se da detenção de uma posição geográfica ou de uma matéria prima, sem as quais o sistema geral não pode funcionar, ou entra em disfunção*" (1984: 57), tendo a consciência de que a actualidade é caracterizada pela era da informação, podemos perceber a informação como matéria-prima.

BIBLIOGRAFIA

Dicionário da Língua Portuguesa. (2006). Porto: Porto Editora.

ANDREW, C., e MITROKHINE, V. (2000). *O Arquivo de Mitrokhine. O KGB na Europa e no Ocidente.* Lisboa: D. Qixote.

BAUER, A., e RAUFER, X. (2002). *A Globalização do Terrorismo.* Lisboa: Prefácio.

BESSA, A. M. (2001). *O Olhar de Leviathan. Uma Introdução à Política Externa dos Estados Modernos.* Lisboa: ISCSP.

BESSA, A. M., e PINTO, J. N. (2001). *Introdução à Política - O poder o Estado e classe política.* Lisboa: Editorial Verbo.

BORAZ, S. C., e BRUNEAU, T. C. (Julho de 2006). Reforming Intelligence. Democracy and Effectiveness. *Journal of democracy, 17*, pp. 28-42.

CAETANO, M. (1967). *Manual de Ciência Política e Direito Constitucional* (5ª ed.). Coimbra: Coimbra Editora.

CAPARINI, M. (2007). Controlling and Overseeing Intelligence Services in Democratic States. In H. Born, e M. Caparini, *Democratic Control of Intelligence Services. Containing Rogue Elephants* (pp. 25-46). Hampshire: Ashgate Publishing Limited.

CARDOSO, P. (2004). *As informações em Portugal.* Lisboa: Gradiva.

CARVALHO, J. S. (2006). Segurança Nacional e Informações. *Segurança e Defesa*, pp. 89-101.

CARVALHO, J. S. (2008). Segurança: Visão Global - A Perspectiva das Informações. *Segurança e Defesa*, 99-104.

CEPIK, M. (2003). *Espionagem e democracia : agilidade e transparência como dilemas na institucionalização de serviços de inteligência.* Rio de Janeiro: Fundação Getúlio Vargas.

CHIAVENATO, I. (2004). *Introdução à Teroria Geral da Administração.* Rio de Janeiro: Elsevier Editora Ltda.

CLARK, R. M. (2004). *Intelligence Analysis. A Target Centric Approach.* Washington: CQ Press.

CLAUSEWITZ, C. V. (1989). *On War.* Princeton: Princeton Unoversity Press.

COUTO, A. C. (1988). *Elementos de Estratégia. Apontamentos para um Curso.* Pedrouços: IAEM.

DIA. (2009). *National Intelligence. A consumer's Guide.* Washington: Defense Intelligence Agency.

DNI. (08 de Março de 2011). *Data Gathering*. Obtido em 16 de Julho de 2011, de Intelligence.gov: http://www.intelligence.gov/about-the-intelligence-community/how-intelligence-works/data-gathering.html

DOUGHERTY, J. E., e PFALTZGRAFF, J. R. (2003). *Relações Internacionais. As Teorias em Confronto.* Lisboa: Gradiva.

ELLIS, W. E. (2010). US Intelligence at the Crossroads. *Mediterranean Quarterly*, 1-11.

ESTEVES, P. (2004). Estado e Informações: Uma Perspectiva Sistémica. In A. Moreira, *Informações e Segurança. Estudos em Honra do General Pedro Cardoso* (pp. 439-458). Lisboa: Prefácio.

FEITH, D. J. (2008). *War and Decision. Inside the Pentagon at the Dawn of the War on Terrorism.* New York: HarperCollins Publishers Inc.

FRATINI, E. (2011). *Mossad. Os carrascos do Kindon.* Lisboa: Bertrand Editora.

FREITAS, M. C. (1989). Conceito. In AAVV, *Enciclopédia Luso-Brasileira de Filosofia. Logos.* Lisboa: Editorial Verbo.

GARCIA, F. P. (Abril-Junho de 2008). A transformação da Intelligence. *Segurança e Defesa*, pp. 103-108.

GAZIT, S. (1989). Intelligence Estimates and the Decision-Maker. In M. I. Handel, *Leaders and Intelligence* (pp. 261-287). Oxon: Frank Cass.

GILL, P., e Phythian, M. (2006). *Intelligence in an Insecure World.* Malden: Polity.

GODSON, R. (1995). Covert Action: Neither Exceptional Tool, Nor Magic Bullet. In R. Godson, E. R. May, e G. Schmitt, *U.S. Intelligence at the Crossroads. Agendas for Reform* (pp. 154-169). Washington: Brassey's.

GOLDMAN, J. (2006). *Words of Intelligence. A dictionary.* Oxford: The Scarecrow Press, Inc.

GOOKINS, A. J. (2008). The Role of Intelligence in Policy Making. *SAIS Review*, 65-73.

GRAY, C. S. (05 de Abril de 2005). *Transformation and Strategic Surprise.* Obtido em 15 de Julho de 2011, de Strategic Studies Institute: http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB602.pdf

HANDEL, M. I. (2004). Leaders and Intelligence. In M. I. Handel, *Leaders and Intelligence* (pp. 3-39). Oxon: Frank Cass.

HERMAN, M. (2004). *Intelligence power in peace and war.* Cambridge: Cambridge University Press.

HULNICK, A. S. (December de 2006). What's Wrong with the Intelligence Cycle. *Intelligence and National Security*, pp. 959-979.

HUNTER, T. B. (25 de Outubro de 2007). *The Chalanges of Intelligence Sharing.* Obtido em 12 de Novembro de 2011, de Operational Studies: http://www.operationalstudies.com/terrorism/TerrorismIntelligencePaper2.pdf

JACKSON, P. (2005). Historical Reflections on the Uses and Limits of Intelligence. In P. Jackson, e J. Siegel, *Intelligence and Statecraft: The Use and Limits of Intelligence in International Society* (pp. 11-52). London: Praeger.

JOHNSON, L. K. (2003). Preface to a Theory of Strategic Intelligence. *International Journal of Intelligence and CounterIntelligence*, 638-663.

JOHNSON, L. K., e WIRTZ, J. J. (2004). *Strategic Intelligence. Windows Into a Secret World.* Los Angeles: Roxbury Publishing Company.

KAMENSKY, J. M., e BURLIN, T. J. (2004). *Collaboration: Using Networks and Partnerships.* Oxford: Rowman & Littlefield Publishers, Inc.

KEAN, T. H. (2004). *The 9/11 commission report.* washington: NCTA.

KEEGAN, J. (2006). *Espionagem na Guerra. Conhecer o Inimigo: De Napoleão à Al-Qaeda.* Lisboa: Tinta da China.

KIRAS, J. D. (2007). The Critical Role of Interagency Cooperation in Countering Suicide Bombings. In J. J. Forest, *Countering Terrorism and Insurgency in the 21st Century. International Perspectives, Volumes 1-3* (pp. 133-150). Westport: Praeger Security International.

LARA, A. S. (2004). *Ciência Política. Estudo da ordem e da Subversão.* Lisboa: Instituto Superior de Ciências Sociais e Políticas.

LERNER, K. L., e LERNER, B. W. (2004). *Encyclopedia of Espionage, Intelligence, and Security.* Farmington Hills: Gale.

Levi, L. (1998). Regime Político. In N. Bobbio, *Dicionário de Política* (pp. 1081-1084). Brasília: Universidade de Brasília.

LEWIS, D. E. (2003). *Presidents and the politics of agency design: political insulation in the United States government bureaucracy, 1946-1997.* Stanford: Stanford University Press.

LOWENTHAL, M. M. (2006). *Intelligence. From Secrets to Policy.* Washington, DC: CQ Press.

MAQUIAVEL, N. (2007). *O Príncipe.* Lisboa: Edições Sílabo.

MINTZ, A., e DeRouen, K. (2010). *Understanding Foreign Policy Making.* Cambridge: Cambridge University Press.

MIRANDA, J. (2002). *Curso de Direito Internacional Público.* Cascais: Principia.

MOREIRA, A. (Abr-Jun de 1984). Hierarquia das Potências: Dependência e Alianação. *Nação e Defesa N.º 30*, pp. 40-60.

MORGENTHAU, H. J., e THOMPSON, K. (1985). *Politics Among Nations. The Struggle For Power And Peace.* New York: McGraw-Hill.

MORUJÃO, A. F. (1985). Função. In AAVV, *Enciclopédia de Filosofia - Logos* (pp. 768-771). Lisboa: Editorial Verbo.

NYE, J. F. (2005). *O Paradoxo do Poder Americano.* Lisboa: Gradiva.

O'BRIEN, K. A. (2007). Covert Action. The "Quiet Option" in International Statecraft. In L. K. Johnson, *Strategic Intelligence* (Vol. III, pp. 23-60). Westport: Praeger Security International.

OSING, F. P. (2007). *Science, Strategy and War. The Strategic Theory of John Boyd.* Oxon: Routledge.

PIRES, C. (1985). Fim. In *Enciclopédia de Filosofia - Logos* (pp. 633-637). Lisboa: Editorial Verbo.

PLESSIS, A.-j. d.-d. (2008). *Testamento Político.* S.L.: Círculo de Leitores.

RENSHON, J., e RENSHON, S. A. (2008). The Theory and Practice of Foreign Policy Decision Making. *Political Psychology, 29, No. 4*, 509-536.

RIBEIRO, H. M. (2008). *Dicionário de Termos e Citações de Interesse Político e Estratégico. Contributo.* Lisboa: Gradiva.

RISEN, J. (2006). *State of War. The Secret History of the CIA and the Bush Administration.* New York: Free Press.

ROMANA, H. B. (2008). Informações: Uma Reflexão Teórica. *Segurança e Defesa*, pp. 98-101.

RUSS, J. (2000). *Dicionário de Filosofia.* Amadora: Didáctica Editora.

S.A. (1998). Números. In S.A., *Bíblia Sagrada* (pp. 207-258). Lisboa: Difusora Bíblica.

SCHMID, G. (2001). *On the existence of a global system for the interception of private and commercial communications (ECHELON interception system).* Bruxelas: European Parliament.

SHAVIT, S. (30 de Outubro de 2010). Um espião confessa-se. (V. Marcelino, Entrevistador)

SHULSKY, A. (1995). What is Intelligence? Secrets and Competition Among States. In R. Godson, E. R. May, e G. Schmitt, *U.S. Intelligence at the Crossroads* (pp. 17-27). Washington: Brassey's.

SHULSKY, A. N., e SCHMITT, G. J. (2002). *Silent Warfare. Understanding the World of Intelligence.* Dulles, Virginia: Potomac Books, Inc.

SIMS, J. E. (2009). A Theory of Intelligence and International Politics. In G. F. Treverton, e W. Agrell, *National Intelligence Systems. Current Research and Future Prospects* (pp. 58-92). Cambridge: Cambridge University Press.

SOUSA, F. d. (2005). *Dicionário de Relações Internacionais.* Santa Maria da Feira: Edições Afrontamento.

TREVERTON, G. F. (2003). *Reshaping National intelligence in an age of information.* Cambridge: Cambridge University Press.

TROY, T. F. (2004). The Quaintness of the U.S. Intelligence Comunity: It's Origin, Theory, and Problems. In L. K. Johnson, e J. J. Wirtz, *Strategic Intelligence. Windows Into a Secret World* (pp. 21-32). Los Angeles: Roxbury Publishing Company.

TZU , S. (2006). *A Arte da Guerra.* Lisboa: Edições Sílabo.

WALTZ, E. (2003). *Knowledge Management in the Intelligence Enterprise.* Norwood: Artech House.

WARNER, M. (2009a). Building a Theory of Intelligence Systems. In G. F. Treverton, *National Intelligence Systems* (pp. 11-37). Cambridge: Cambridge University Press.

_____ (2009b). Intelligence as risk Shifting. In P. Gill, S. Marrin, e M. Phythian, *Intelligence Theory. Key Questions and Debates* (pp. 16-32). London: Routledge.

WETTERING, F. L. (2010). Counterintelligence. The Broken triad. In C. Andrew, R. Aldrich, e W. Wark, *Secret Intelligence. A reader* (pp. 281-308). London: Routledge.

WILLIAMS, P. D. (2008). *Security Studies. An Introduction.* New York: Routledge.