

***INSTITUTO DE ALTOS ESTUDOS MILITARES***  
***CURSO DE ESTADO-MAIOR***

***(2003/2005)***



***TRABALHO INDIVIDUAL DE LONGA DURAÇÃO***

***Métodos e factores de análise às ameaças à Segurança e  
à Defesa Nacional***

***João Pedro Pereira Bastos Rocha***  
***Maj Tm (Engº)***

***Presidente do Júri: Maj Gen Ferreira da Silva***  
***Arguente Principal: Cor Art (Tir) Rodrigues Viana***  
***Arguente: TCor Eng Vale Couto***  
***Arguente: Maj Inf Amaral Lopes***  
***Arguente: Maj Inf Valente Marques***

**ESTE TRABALHO É PROPRIEDADE DO INSTITUTO DE ALTOS  
ESTUDOS MILITARES**

***ESTE TRABALHO FOI ELABORADO COM FINALIDADE  
ESSENCIALMENTE ESCOLAR, DURANTE A FREQUÊNCIA  
DE UM CURSO NO INSTITUTO DE ALTOS ESTUDOS  
MILITARES, CUMULATIVAMENTE COM A ACTIVIDADE  
ESCOLAR NORMAL. AS OPINIÕES DO AUTOR, EXPRESSAS  
COM TOTAL LIBERDADE ACADÉMICA, REPORTANDO-SE  
AO PERIODO EM QUE FORAM ESCRITAS, PODEM NÃO  
REPRESENTAR DOCTRINA SUSTENTADA PELO INSTITUTO  
DE ALTOS ESTUDOS MILITARES.***

PROFESSOR ORIENTADOR:

Amaral Lopes

Maj Inf

---

**Métodos e factores para a análise das ameaças à  
Segurança e à Defesa Nacional**

**Instituto de Altos Estudos Militares**  
Lisboa, Janeiro de 2005

## Resumo

Combater novas ameaças assimétricas como o terrorismo, o crime organizado e a lavagem de dinheiro, requer um sistema de Informações ágil que actue de forma activa e que faça uso das mais avançadas tecnologias de informação e comunicação.

Neste trabalho apresentamos as profundas alterações ocorridas no contexto estratégico internacional e a emergência de novas ameaças. O colapso do Pacto de Varsóvia equipara-se, no surgimento de novas ameaças, à abertura da caixa de Pandora, muitos conflitos latentes explodiram com o fim do mundo bipolar. Surgiram actores não estatais que criam novos desafios aos serviços de Informações. Estes escancaram-se com a premência de novas formas de identificar as ameaças e a urgência da implementação de novos sistemas computacionais para analisar todos os dados armazenados.

As técnicas de *data mining* e análise automática de dados são ferramentas poderosas, que ajudam ao combate das novas ameaças, e que se encontram disponíveis para serem implementadas pelos Serviços de Informações. Todavia são ferramentas que também geram controvérsia e preocupações, pois apesar de fazerem uma análise de dados de forma fiável e eficaz, entram em conflito com o direito à privacidade.

A adopção de sistemas de *data mining* pode ser a resposta a estes novos desafios. O presente estudo aborda as necessidades de implementação destes sistemas, as preocupações e receios que podem ser geradas e as soluções, ao nível da tecnologia, para os minimizar. Concluimos que, embora estas técnicas sejam muito poderosas, é um erro olhá-las como soluções completas para os problemas de Segurança, uma vez que é impossível eliminar, completamente a subjectividade na análise da informação.

## **Abstract**

Defeating new assymmetrical threats such as terrorism, organized crime and money laundering, requires a more nimble Intelligence apparatus that operates more actively and makes use of advanced information and communication technology.

In this study we present the profound alterations that have occurred in the international strategic enviroment and the appearance of new threats. We can compare the collapse of the Warsaw Pact, in the sprouting of new threats, to the opening of Pandora's box; many latent conflicts have blown up with the end of the bipolar world. Non-state players have appeared and have caused new intelligence challenges. Intelligence were confronted with the need to adopted new approaches to identifying the threats and the necessity to implement new information technology systems to analyze all stored data.

Data mining and automated data analysis techniques are powerful tools that help to defeat new threats, and are avaiable to be implemented in intelligence services. However these tools also generate controversy and concern, due to the fact that they make the analysis of data - including private data – easier and more powerful.

The adoption of data mining systems can be the response to these new challenges. This study tackles the necessities of the implementation of these systems, the concerns and distrust that can be generated and the technology-related solutions, to minimize them. We conclude that even though these techniques are very powerful, it is an error to look at them as complete solutions to security problems.

## **Dedicatória**

À Fátima, à Beatriz e ao Nuno.  
Pelo estímulo e dedicação.

## Abreviaturas e acrónimos

AAP	<i>Allied Administrative Publications</i> (NATO)
ADM	Armas de destruição maciça
BISM	Batalhão de Informações e Segurança Militar
CEDN	Conceito Estratégico de Defesa Nacional
CEM	Conceito Estratégico Militar
Cor	Coronel
CRP	Constituição da República Portuguesa
DARPA	<i>Defense Advanced Research Projects Agency</i>
EEINC	Espaço Estratégico de Interesse Nacional Conjuntural
EEINP	Espaço Estratégico de Interesse Nacional Permanente
ETA	Grupo separatista Basco ( <i>Euskadi Ta Askatasuna</i> )
EUA	Estados Unidos da América
FA	Forças Armadas
HUMINT	Informações obtidas por pesquisa humana ( <i>Human Intelligence</i> )
IAEM	Instituto de Altos Estudos Militares
IAO	<i>Information Awareness Office</i>
IPCE	Instituto Português de Conjuntura Estratégica
IPRI	Instituto Português de Relações Internacionais
IRA	Exército Republicano Irlandês
IWG	<i>Intelligence Working Group</i>
KDD	Descoberta de conhecimento em bases de dados ( <i>Knowledge Discovery in Databases</i> )
LDNFA	Lei da Defesa Nacional e das Forças Armadas
Maj	Major
MC	<i>Military committee</i>
MEDN	Ministro de Estado e da defesa Nacional
NATO	<i>North Atlantic Treaty Organisation</i> , o mesmo que OTAN
NIWS	<i>Nato Intelligence Warning System</i>
ONU	Organização das Nações Unidas
OSCE	Organização para a Segurança e Cooperação na Europa
OSINT	Informações obtidas por fontes abertas ( <i>Open source Intelligence</i> )

OTAN	Organização do Tratado do Atlântico Norte, o mesmo que NATO
PGR	Procuradoria Geral da República
SIEDM	Serviço de Informações Estratégicas de Defesa e Militares
SIRP	Serviço de Informações da República Portuguesa
SIS	Serviço de Informações de Segurança
TCor	Tenente Coronel
TECHINT	Informações obtidas por meios técnicos ( <i>Technical Intelligence</i> )
TGen	Tenente General
TIA	<i>Terrorism Information Awareness</i>
TIC	Tecnologias de Informação e Comunicação
UE	União Europeia
URSS	União das Repúblicas Socialistas Soviéticas

## Índice

Introdução.....	9
I – Quadro Legal de Referência.....	15
I. 1 Constituição da República.....	15
I. 2 Sistema de Informações da República Portuguesa.....	17
II – Segurança e Defesa Nacional: conceitos em mudança.....	18
II. 1 Um novo ambiente estratégico.....	18
II. 2 Segurança e Defesa Nacional.....	19
II. 3 Síntese conclusiva.....	22
III – As ameaças.....	24
III. 1 Conceito de ameaça.....	24
III. 2 Velhas e novas ameaças.....	25
III. 2. 1 Velhas ameaças.....	25
III. 2. 2 Novas ameaças.....	26
III. 3 O CEDN e as ameaças externas a Portugal.....	28
III. 4 Síntese conclusiva.....	29
IV – O Papel das Informações.....	30
IV. 1 Informações e poder do Estado.....	30
IV. 2 A necessidade de Informações.....	31
IV. 3 O SIRP.....	32
IV. 4 Síntese conclusiva.....	33
V – Métodos e factores para análise das ameaças.....	35
V. 1 Conceito de indicadores e avisos.....	35
V. 2 Métodos de análise.....	36
V. 3 O NIWS.....	37
V. 4 Síntese conclusiva.....	39
VI. Um método proposto: análise de dados com data mining.....	41
VI. 1 Conceito de <i>Data Mining</i> .....	41
VI. 1. 1 Análise por assuntos ou ligações.....	42
VI. 1. 2 Análise de padrões.....	43
VI. 2 O Processo.....	44
VI. 2. 1 Recolha e processamento de dados.....	45
VI. 2. 2 Modelos de pesquisa.....	46

VI. 2. 3 Avaliação e tomada de decisão .....	47
VI. 3 Riscos .....	48
VI. 3. 1 O fim da “privacidade”?.....	49
VI. 3. 2 Falsos positivos e falsos negativos .....	50
VI. 3. 3 Uso inadequado da Informação .....	51
VI. 4 Atenuar os riscos .....	52
VI. 5 O estado da arte .....	54
VI. 6 Síntese conclusiva .....	55
VII. Conclusões .....	57
Bibliografia.....	61
Índice de Apêndices .....	68
Índice de Anexos .....	69

Knock, knock.  
“Who’s there?”  
“FBI. You’re under arrest.”  
“But I Haven’t done anything.”  
“You will if we don’t arrest you,” replied Agent Smith of the Precrime Squad.<sup>1</sup>

## INTRODUÇÃO

Em consequência das dramáticas alterações verificadas na ordem mundial desde o fim da guerra-fria, quer a nível político, estratégico, económico, cultural e de globalização da informação, os Estados deparam-se com novas ameaças à sua Segurança e novos desafios à sua soberania.

As alianças militares e económicas em que Portugal se encontra inserido, nomeadamente a NATO, bem como o desanuviamento ocorrido em virtude do colapso do Pacto de Varsóvia, deixam entrever como remota a ameaça à integridade do território nacional. Todavia, num mundo de assimetrias, surgem novas ameaças de cariz multifacetado que colocam novos desafios e exigem alterações significativas à forma de pensar e de actuar dos responsáveis pela Segurança Nacional.

No período da guerra fria era relativamente simples identificar as ameaças e as necessidades de Informações. Poderia ser difícil obter a informação necessária, mas o que se procurava era bem claro: conhecer as movimentações da outra superpotência, as suas possibilidades reais e as suas intenções. Actualmente as ameaças assimétricas são caracterizadas por colocarem graves escolhos aos Serviços de Informações. Ameaças como o terrorismo, o crime organizado altamente violento, o tráfico de armas, produtos radioactivos e de pessoas, são perpetradas por indivíduos sem escrúpulos, difíceis de identificar, organizadas em redes complexas e com o objectivo, que vai para além do meramente económico e político, e chega mesmo a ter em vista destruir o nosso modo de vida. O trabalho dos Serviços de Informações é colossal. Tem que encontrar estes criminosos num “oceano de ruído”, compreender os seus padrões de actuação e desenvolver meios para prevenir as suas acções.

Creemos que a tecnologia pode dar um contributo decisivo neste árduo trabalho. É necessário encontrar novas formas mais inteligentes e eficientes de colecta e análise de dados, deve-se garimpar a informação para encontrar “pontos” que, depois de unidos, forneçam uma imagem fiável das actividades que procuramos. É imperativo transformar

---

<sup>1</sup> Ver filme Relatório Minoritário, 20<sup>th</sup> Century Fox 2002. Citado por TAIPALE, K. A., *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, in Science and Technology Law Review, Columbia, Vol. V, 2003, p. 4. Disponível em [www.stlr.org](http://www.stlr.org).

informação em conhecimento, em tempo útil, criar normas legais de análise e disseminação da Informação para se obterem novas opções na prevenção das ameaças. As técnicas de *data mining* são uma ajuda fundamental que, garantindo a privacidade e a segurança, podem contribuir para uma melhor avaliação das ameaças.

O presente trabalho situa-se na área da Estratégia e na área das Informações. É na área de avaliação das ameaças à Segurança Nacional que Portugal deverá efectuar um esforço intenso para adoptar as modalidades de acção estratégica que possam racionalizar os meios para fazer face às ameaças e atingir os seus objectivos, salvaguardando os seus interesses.

### **Definição e objectivo da Investigação**

Face ao tema proposto, “Métodos e factores para a análise das ameaças à Segurança e à Defesa Nacional”, pretendemos fazer uma compilação dos principais problemas de análise das novas ameaças contribuindo para a criação de um conjunto de ferramentas que apoiem uma política de Informações ágil e eficaz no quadro das ameaças que afectam Portugal e países aliados. Desta forma, pretendemos que o nosso estudo possa determinar um conjunto de requisitos necessários à implementação de um modelo de análise automática de dados, baseada em padrões, contemplando as garantias de segurança da informação e as garantias e liberdades dos cidadãos.

### **Importância do estudo**

A proposta de realização deste estudo, partiu da nossa percepção que as ameaças que se colocam aos Estados são difusas e difíceis de analisar pelos métodos tradicionais do período da chamada guerra fria. Por um lado, a análise da informação efectuada pelos serviços de Informações é sempre alvo de especulação e de receios por parte da comunidade em geral, dado o factor de poder que apresentam dentro do Estado. Por outro lado, o volume de informação disponível é tão grande que a sua análise, por parte de analistas convencionais, é uma tarefa impossível sem o auxílio de modernas técnicas de análise automática de dados e de *data mining*.

A actualidade e pertinência deste estudo parece-nos bem patente no novo Conceito Estratégico de Defesa Nacional (CEDN) em que as novas ameaças são apontadas como ameaças externas, inserindo-se claramente nas missões da Forças Armadas.

## **Delimitação do estudo**

Dada a natureza académica deste trabalho, delimitaremos o presente estudo à análise das necessidades estruturais e implicações legais da actuação dos Serviços de Informações, no levantamento de um sistema de *data-mining* e de análise automática de dados, que possa responder ao processamento de um grande volume de informações baseadas em pesquisas por padrão e em pesquisas por assunto.

## **Corpo de Conceitos**

Entendemos enunciar, desde já, um conjunto de conceitos e definições a que faremos referência ao longo do presente estudo. Esta decisão prende-se com a existência de conceitos em que as traduções possam ser passíveis de diferentes interpretações e pretende clarificar as definições na área de estudo da Estratégia. Apresentaremos os conceitos agrupados em áreas afins e, sempre que julgamos necessário, apresentaremos uma explicação do termos.

Risco – Perigos a que os interesses estratégicos de um Estado ou coligação podem estar sujeitos. Estes riscos, que são riscos à estabilidade e à segurança, não são, necessariamente, originados dentro ou na vizinhança do Estado ou coligação.<sup>2</sup>

Ameaça – “Qualquer acontecimento ou acção (em curso ou previsível) que contraria a consecução de um objectivo e que, normalmente, é causador de danos, materiais e morais.”<sup>3</sup>

Os conceitos de Defesa Nacional e de Segurança Nacional serão abordados de forma mais exaustiva no Capítulo II, pois como afirma o Coronel Viana, “as exigências do novo ambiente de segurança, acentuadas pelos acontecimentos de 11 de Setembro, têm vindo a consolidar a adopção de conceitos mais amplos de segurança que transcendem a área tradicional da defesa.”<sup>4</sup>

Defesa Nacional – É o conjunto de medidas tanto de carácter militar como político, económico, social e cultural que, adequadamente coordenadas, integradas e desenvolvidas, global e sectorialmente, permitem reforçar a potencialidade da Nação e

---

<sup>2</sup> Nato Intelligence Warning System MC 166, NATO, 2004

<sup>3</sup> COUTO, Abel Cabral, *Elementos de Estratégia – apontamentos para um curso*, Vol. 1, IAEM, Lisboa, 1998, p. 329.

<sup>4</sup> VIANA, Rodrigues, *O conceito de segurança alargada e o seu impacto nas missões e organização das forças armadas*, TILD, CSCD, IAEM, 2003, p. 1.

minimizar as suas vulnerabilidades, com vista a torná-la apta a enfrentar todos os tipos de ameaça que, directa ou indirectamente, possam pôr em causa a Segurança Nacional.<sup>5</sup>

Segurança Nacional – É a condição da Nação que se traduz pela permanente garantia da sua 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 de democráticas.<sup>6</sup>

A análise das ameaças é uma das actividades dos Serviços de Informações que trabalham a informação em bruto. Os conceitos que se apresentam de seguida, informação e Informações (*Intelligence*), são de difícil separação em Português. No capítulo IV apresentaremos uma clarificação do papel das Informações na actividade de segurança do Estado. Neste trabalho iremos usar a expressão Serviços de Informaç ou apenas Informação, com letra maiúscula, para traduzir “*intelligence*” e distinguir de informação no seu sentido amplo.

Informações (*Intelligence*) – “É o produto resultante do processamento de informação relativa a nações estrangeiras, hostis ou forças ou elementos potencialmente hostis, ou áreas de presentes ou potenciais operações. O termo é também aplicado à actividade que dá origem a informações, e como termo genérico, àqueles que levam a cabo o processo que conduz à sua produção”.<sup>7</sup>

Informação – Dados não processados de todos os elementos que podem ser usados na produção de Informações.<sup>8</sup>

No âmbito da análise das Informações vamos apresentar os conceitos de indicador e de aviso, que serão aprofundados no capítulo V.

Indicador – Uma acção ou condição, específica ou generalizada, que se pode esperar que preceda acontecimentos que podem ser prejudiciais.

Aviso – A comunicação e confirmação de uma ameaça, risco ou preocupação implícita numa vasta gama de actividades. Um aviso não é considerado realizado até que seja tomada uma decisão por parte da entidade competente.

---

<sup>5</sup> RAMALHO, TGen Pinto, “A crise Internacional – a sua Gestão”, in *Estratégia*, Vol. XII, ed. IPCE, Lisboa, 2000, pp. 171-172.

<sup>6</sup> Cf. Op. Cit., RAMALHO, 2000, 172.

<sup>7</sup> NATO Glossary of Terms and Definitions, AAP-6, 2004, p. 2-I-5.

<sup>8</sup> AAP-6, 2004, p. 2-I-3.

*Data mining*<sup>9</sup> – Processo de extrair informação válida, previamente desconhecida e finalmente compreensível a partir de grandes bases de dados, e da sua utilização no processo de tomada de decisões.

*Data Warehouse* – “Base de dados analítica orientada por assuntos, integrada, variável com o tempo mas não volátil, com o objectivo de dar suporte ao processo da tomada de decisão.”<sup>10</sup>

## Metodologia

O nosso percurso metodológico iniciou-se efectuando uma pesquisa bibliográfica e documental (legislação e documentos militares) sobre o tema em questão, nomeadamente a nível nacional, dos EUA e da OTAN. Em seguida, definiu-se a questão central que guia a nossa investigação: “Quais as implicações da implementação de um sistema de *data mining* para a análise às ameaças à Segurança e à Defesa Nacional?”.

Deduzidas as questões derivadas a partir da questão central, a nossa metodologia baseia-se, essencialmente, no estudo dos modelos lançados nos EUA e da sua aplicabilidade à realidade nacional, com vista à definição de um modelo que possa ser implementado em Portugal. Como complemento efectuaram-se entrevistas a reconhecidos especialistas na matéria que se encontram referidas na bibliografia.

As agressões terroristas ocorridas nos EUA, nas embaixadas ou navios de guerra, que contribuíram para os colocar na posição de liderança de projectos de reestruturação do Serviços de Informações, nomeadamente nos projectos de *data mining* e de análise automática de informação, fundamentam o nosso trabalho.

As hipóteses orientadoras do nosso estudo foram levantadas com base na nossa percepção e nas entrevistas realizadas, e são:

- *O quadro legal dos Serviços de Informação encontra-se desactualizado face às características das novas ameaças;*
- *O processamento automático de informação usando o data mining, pode ser efectuado sem ferir a privacidade dos cidadãos;*

---

<sup>9</sup> Não iremos usar qualquer tradução para Português deste termo devido à falta de normalização por parte da comunidade científica. No Brasil alguns autores usam a expressão “mineração de dados” como tradução. O mesmo será efectuado com o termo *data warehouse*.

<sup>10</sup> VIEIRA, José António da Silva, *O Sistema de Apoio à Decisão de Gestão no Exército Português. Contributos para um modelo mais operacional e eficaz*, TILD, Lisboa, IAEM, 2002. p. V.

- *O actual sistema nacional de análise de Informação não corresponde às necessidades de actuação preventiva, colocando Portugal em igualdade com os seus parceiros na UE e na OTAN.*

### **Organização e Conteúdo do Estudo**

O presente trabalho está organizado em Introdução, seis capítulos e Conclusões. Após uma breve Introdução, dedicamos um primeiro capítulo à análise do quadro legal que enquadra as missões das FA e das actividades de Informações.

No segundo capítulo analisaremos a nova realidade da conflitualidade mundial e as alterações por ela provocadas nos conceitos de segurança e defesa.

Um Estado deve estar pronto para responder em tempo oportuno às ameaças ou agressões que se lhe deparam. Este quanto melhor conseguir avaliar as ameaças, mais oportunamente pode criar mecanismos para as enfrentar e evitar que se concretizem numa agressão, garantindo a segurança e o bem-estar da população. As ameaças que se colocam abrangem todo o espectro da vida dos Estados. Podem ser militares, económicas, de crime organizado, terroristas, ambientais e ainda, de carácter político. No capítulo III vamos caracterizar cada tipo de ameaças.

No quarto capítulo vamos debruçarmo-nos sobre o papel das Informações, nomeadamente o enquadramento global do SIRD.

Nos quinto e sexto capítulos iremos focar a nossa atenção sobre os métodos para análise de ameaças e os seus factores determinantes. Começaremos por visitar os métodos tradicionais para depois expor os desenvolvimentos mais recentes na área de descoberta de conhecimento em bases de dados. Pretendemos discorrer sobre as suas imensas potencialidades, mas também sobre os riscos, ressaltando as liberdades e garantias das sociedades democráticas.

Concluiremos o nosso estudo apresentando as propostas para uma possível implementação de um sistema usando o *data mining* no SIRD.

## **I – QUADRO LEGAL DE REFERÊNCIA**

A actividade de Informações tem um quadro legal complexo, encontrando-se disperso por vários diplomas legais e está num período de alterações. Face a esta situação, procurou-se reunir a legislação mais importante para construção do nosso quadro legal de referência, no âmbito de actuação das Forças Armadas no quadro de novas ameaças. Seguidamente, iremos abordar os tópicos legislativos mais relevantes para o nosso estudo.

- Lei constitucional n.º 1/2004, 24 de Julho – Constituição da República Portuguesa (CRP) (6ª Revisão).
- Lei n.º 29/82, 11 de Dezembro, com seis alterações posteriores – Lei da Defesa Nacional e das Forças Armadas (LDNFA);
- Lei n.º 20/87, de 12 de Junho, alterada pela Lei n.º 8/91, de 1 de Abril – Lei de Segurança Interna.
- Lei n.º 30/84, de 5 de Setembro, alterada pelas Leis n.ºs 4/95, de 21 de Fevereiro, 15/96, de 30 de Abril, e 75-A/97, de 22 de Julho – Lei-quadro do Sistema de Informações da República Portuguesa (SIRP)
- Lei n.º 15/96, de 30 de Abril – Reforça as competências do Conselho de Fiscalização dos Serviços de Informações.
- Decreto-Lei n.º 254/95, 30 de Setembro – Lei Orgânica do Serviço de Informações Estratégicas de Defesa e Militares (SIEDM);
- Decreto-Lei n.º 225/85, de 4 de Julho, alterado pelos Decretos-Leis n.º 369/91, de 7 de Outubro, e 245/95, de 14 de Setembro – Lei Orgânica do Serviço de Informações de Segurança (SIS).
- Decreto-Lei n.º 48/93, de 26 de Fevereiro – Lei Orgânica do Estado-Maior-General das Forças Armadas.
- Resolução do Conselho de ministros n.º 6/2003 – CEDN.
- Resolução do Conselho de Ministros n.º 22/98 – Regulamento do Centro de Dados do SIEDM.
- Conceito Estratégico Militar – Aprovado pelo MEDN, 22 de Dezembro 2003.

### **I. 1 Constituição da República**

A CRP no seu artigo 273º determina que, “a defesa nacional tem por objectivos garantir, no respeito da ordem constitucional, das instituições democráticas e das

convenções internacionais, a independência nacional, a integridade do território e a liberdade e a segurança das populações contra qualquer agressão ou ameaça externas.” Afirmo no seu n.º 1 do artigo 275º que “às Forças armadas incumbe a defesa militar da República.”

Uma análise restrita à CRP leva-nos a constatar que as actividades de Defesa Nacional só são executadas se existir uma ameaça ou agressão externa. Coloca-se o problema de actuação das Forças Armadas em situações em que exista uma ameaça ou agressão, ainda que por elementos externos, que actuem no interior do território nacional. Num ambiente estratégico complexo, que será caracterizado no capítulo seguinte, importa contextualizar o papel das FA no quadro dos equilíbrios constitucionais de forças e poderes, de acordo com o citado artigo 273º em oposição ao disposto no artigo 272º que define as missões de polícia. A necessidade de esclarecer esta situação levou o Ministro da Defesa Nacional a solicitar ao Conselho Consultivo da Procuradoria Geral da República (PGR) que se pronunciasse, tendo ficado claro que os conceitos de agressão ou ameaça externa são indeterminados e não podem deixar de ser actualizados.<sup>11</sup>

Decorrente desta necessidade de equilíbrio de poderes e definição das missões das FA e das forças de segurança o governo explicitou, no novo CEDN, quais as ameaças externas que se enquadram no cumprimento das missões das FA. No Capítulo III faremos uma análise destas ameaças.

---

<sup>11</sup> Transcrevemos do Parecer da PGR n.º 147/2001, publicado no DR n.º 40 de 16 de Fevereiro de 2002, que enquadra, nas conclusões, a actuação das FA em missões de prevenção de terrorismo e ameaças NBQ:

- «1 - A Constituição da República Portuguesa comete às Forças Armadas a missão primária e nuclear de defesa militar da República (n.º 1 do artigo 275.º da CRP), com vista a garantir a “independência nacional”, a “integridade do território” e a “liberdade e a segurança das populações contra qualquer agressão ou ameaça externas”.
- 2 – Os conceitos de “agressão” e “ameaça” externas são conceitos indeterminados que não podem deixar de ser objecto de uma integração actualista, de modo a abranger novas formas de actuação externa susceptíveis de afectar os bens jurídicos que constituem objecto do conceito constitucional de defesa nacional.
- 3 – Perante uma agressão ou ameaça do exterior, que pelo seu significado e dimensão afecte de forma séria e fundada os bens jurídicos objecto do conceito constitucional de defesa nacional, a defesa militar poderá envolver uma componente externa, caracterizada pelo exercício de um direito de legítima defesa, no quadro dos compromissos internacionais e, uma componente interna, dirigida à estrita protecção dos mesmos bens jurídicos contra ameaças externas, dentro do espaço físico do território nacional (n.º 2 do artigo 273.º da CRP, conjugado com o n.º 1 do artigo 2.º da LDNFA).
- 4 – A defesa militar perante ameaças externas ao funcionamento de sectores de produção e abastecimento alimentar, industrial e energético, dos transportes e das comunicações, na medida em que constituem interesses vitais para o bem-estar e segurança das populações, compreende-se na previsão do n.º 2 do artigo 273.º da CRP e no n.º 1 do artigo 2.º da LDNFA.»

## **I. 2 Sistema de Informações da República Portuguesa**

As actividades de informações são reguladas pela lei-quadro do SIRP que estrutura o Sistema de Informações da República Portuguesa, criando os órgãos que o integram e definindo os princípios fundamentais da sua organização, do seu funcionamento e da sua articulação de forma a assegurar, no respeito da Constituição e da lei, a produção de Informações necessárias à salvaguarda da independência nacional e à garantia da segurança interna.

Os artigos 19º e 20º da lei-quadro do SIRP, definem as funções do SIEDM e do SIS. O SIEDM fica vocacionado para a produção de informações no âmbito da segurança externa de Portugal e para a segurança militar<sup>12</sup>, deixando ao SIS a responsabilidade de produção de Informações que garantam a segurança interna e a prevenção da sabotagem, do terrorismo, da espionagem que possam afectar o Estado de Direito. No apêndice 1 encontra-se a orgânica do SIRP. No IAEM têm-se desenvolvido vários trabalhos sobre um modelo do SIRP para o futuro, considerando uma nova tipologias de ameaças. No capítulo IV em que abordaremos o Papel das Informações, chamaremos a atenção para as propostas que considerarmos mais prementes.

De acordo com o art.º 23, da lei-quadro do SIRP, o SIS e o SIEDM podem ter centros de dados, regulados por diploma próprio, mas cada centro de dados funciona autonomamente, não podendo ser conectado com o outro.

Numa análise objectiva da lei sobre as Informações em Portugal, ressalta a ideia de uma enorme estanquicidade nas actividades de cada serviço, faltando um órgão que possa congrega a Informação dos diferentes serviços.

---

<sup>12</sup> Transcrevemos parte dos artigos 19.º e 20.º da lei quadro do SIRP: (sublinhado do autor)

“Artigo 19º (Serviço de Informações Estratégicas de Defesa e Militares)

1 - O Serviço de Informações Estratégicas de Defesa e Militares é o organismo incumbido da produção de informações que contribuam para a salvaguarda da independência nacional, dos interesses nacionais, da **segurança externa do Estado Português**, para o cumprimento das missões das Forças Armadas e para a segurança militar.

Artigo 20º (Serviço de Informações de Segurança)

1 - O Serviço de Informações de Segurança é o organismo incumbido da produção de informações que contribuam para a salvaguarda da **segurança interna e a prevenção da sabotagem, do terrorismo**, da espionagem e a prática de actos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido.”

“Les intérêts stratégiques des États, en ce début du XXI<sup>e</sup> siècle, ont complètement changé. Les risques ne sont plus les mêmes, et les solutions à trouver n’ont souvent rien à voir avec la chose militaire.”<sup>13</sup>

Ignacio Ramonet

## II – SEGURANÇA E DEFESA NACIONAL: CONCEITOS EM MUDANÇA

### II. 1 Um novo ambiente estratégico

Com o fim da guerra fria e os ataques de 11 de Setembro o ambiente estratégico internacional sofreu profundas transformações. Autores de todos os quadrantes políticos, de todos os países, tentam caracterizar uma nova ordem mundial, perceber a sua racionalidade, a sua legitimidade e a sua estabilidade. O General Loureiro dos Santos afirma que “com os acontecimentos do 11 de Setembro de 2001, começou a Idade Imperial”, referindo que o período, entre a queda do muro de Berlim, em 1989, e os ataques aos EUA, foi de revelação das profundas alterações da velha ordem mundial bipolar.<sup>14</sup> O mundo está perante um novo ambiente estratégico que assenta numa globalização abrangente de todas as actividades da vida humana, na emergência de conflitos não clausewitzianos, nas dificuldades de regulação do controlo das armas de destruição maciça (ADM) e na alteração das tipologias das crises internacionais.

A par de grandes vantagens para a economia mundial, a globalização também afectou os fenómenos terroristas, o crime organizado, a lavagem de dinheiro, o tráfico de pessoas, os cyber crimes, etc.. O Coronel Viana refere que “num mundo marcado pela interdependência estrutural das relações internacionais e pelo fenómeno do transnacionalismo, assistiu-se a uma alteração qualitativa da natureza das ameaças e riscos.” “À semelhança do que aconteceu com a economia, as ameaças globalizaram-se”.<sup>15</sup> Guéhenno reforça esta ideia, afirmando que a “grande novidade do século XXI resulta da interacção muito forte entre todas as partes do mundo. Elas estão ligadas umas às outras, mas, ao mesmo tempo não se podem controlar.”<sup>16</sup>

Muita da actual conflitualidade no mundo pode correr o risco de se eternizar, alimentada pelos lucros de actividades ilícitas e pelo aparecimento dos chamados “estados falhados”, perturbadores regionais e refúgio de organizações terroristas e

---

<sup>13</sup> RAMONET, Ignacio, *Des nouveaux intérêts stratégiques* in *Les Guerres qui menacent le monde*, Éditions du Félin, Paris, 2001, p. 55.

<sup>14</sup> SANTOS, José Alberto Loureiro dos, *A Idade Imperial: a nova era, Reflexões sobre Estratégia III*, Mem Martins, Ed. Publicações Europa-América, 2003, p. 85.

<sup>15</sup> Op. Cit., VIANA, 2003, 3.

<sup>16</sup> Cf. GUÉHENNO, Jean-Marie, *Sécurité et globalisation* in *Les Guerres qui menacent le Monde*, Ed. Du Félin, 2001, Paris, p. 93

criminosas,<sup>17</sup> emergindo na cena internacional actores “não clausewitzianos”. Estes actores não pretendem a confrontação directa entre Estados, nem aceitam as regras do jogo da comunidade internacional, antes querem impor as suas regras, obter lucros avultados, aproveitando as vulnerabilidades das sociedades desenvolvidas, e emergir, no futuro, como actores de cariz político usando o sofisma do fundamentalismo religioso como argumento da sua actuação.

A terceira característica de um novo ambiente estratégico prende-se com a dificuldade no controlo das ADM. A implosão da ex-URSS veio trazer para a comunidade internacional um conjunto de países com capacidade nuclear instalada mas sem capacidade, quer tecnológica quer económica, de controlo dessas armas. Os EUA têm feito um esforço imenso de apoio à não proliferação dos materiais para fabrico de ADM, nomeadamente apoiando financeiramente a Rússia na manutenção das infra-estruturas de produção de plutónio enriquecido.

As alterações na nova conflitualidade, em conjunto com alterações significativas em conceitos tão enraizados como a soberania e as fronteiras geográficas, levam a que os Estados tenham necessidade de se adaptar a novos cenários e responder a novas ameaças e riscos, de concretização imprevisível, de carácter multifacetado e transnacional.

O CEDN sublinha que neste novo ambiente estratégico as ameaças tradicionais de cariz militar têm-se atenuado, e “a maximização dos princípios da surpresa e da decepção, num combate assimétrico por actores não tradicionais, onde se insere o terrorismo transnacional, a par da demonstração de capacidade e de motivação, por parte de organizações mal definidas e não totalmente identificadas, para levar a efeito acções de grande impacto, configuram a possibilidade de eclosão de elevados níveis de destruição humanos e materiais. As consequências de tais acções nas economias, na segurança e na estabilidade internacionais, transcendem a capacidade de resposta individualizada dos Estados e interrelacionam os conceitos de segurança interna e externa e os objectivos que estes prefiguram.”<sup>18</sup>

## **II. 2 Segurança e Defesa Nacional**

Com o advento de uma nova ordem mundial, ainda com contornos pouco definidos, as actividades de segurança dos Estados sofreram profundas alterações, pois

---

<sup>17</sup> GASPAR, Carlos, *O regresso do realismo*, IPRI, disponível em <http://www.ipri.pt/investigadores/artigo.php?idi=3&ida=48>

<sup>18</sup> CEDN, p. 2

as ameaças tradicionais tornaram-se improváveis e surgiram novas ameaças de natureza difusa. No capítulo seguinte iremos abordar uma classificação das ameaças que se apresentam no novo contexto estratégico, sendo de realçar que a política mundial tem sido marcada pelas ondas de choque dos atentados terroristas de 11 de Setembro de 2001, nos EUA, e de 11 de Março de 2004 em Espanha. Isto veio alterar a percepção dos Estados sobre a sua segurança e quais os meios para fazer face às novas ameaças que se revelam.

Historicamente a segurança dos Estados está dividida em segurança interna e em segurança externa. As forças e serviços de segurança estão vocacionados para lidar com os aspectos da segurança interna enquanto que às Forças Armadas compete a responsabilidade da segurança externa.<sup>19</sup> Como afirma a Dra. Mafalda Borges, “a distinção clássica entre segurança interna e Defesa Nacional, entendida como Segurança Externa, é questionada constantemente dado o evoluir da reorganização geoestratégica da hegemonias políticas e económicas da Ásia, Europa e América do Norte e das ameaças transnacionais colocadas, já não por Estados-nação (sujeitos tradicionais de direito internacional), mas por indivíduos e grupos ou associações criminosas.”<sup>20</sup> Ou seja, para se atingir um dos objectivos últimos de uma unidade política – garantir a Segurança – é necessário um conjunto de políticas de Segurança Nacional que reúna os principais sectores de acção do Estado numa estratégia concertada e unificada. A ideia de uma Segurança Nacional é uma concepção única e indivisível em aspectos externos e internos. Os cidadãos querem viver em segurança, não valorizando mais se a sua inexistência se dever a actores externos ou internos do Estado.

No âmbito nacional as ameaças que se apresentam adoptam um cariz de “novidade” devendo ser abordadas também de uma forma que não a tradicional. A actuação das entidades responsáveis pela Segurança deverá ser orientada de forma a poder responder às solicitações que se colocam. O Coronel Viana frisa que “a natureza destas ameaças não é compaginável com a separação hoje existente entre as componentes interna e externa da Segurança Nacional. Na actual conjuntura, revela-se como inadequado e arriscado tentar configurar ameaças ou riscos numa óptica rigidamente compartimentada de que uns são um problema de “segurança” e outros um problema de “defesa” e, como tal, deverem ser tratados distintamente pelas Forças de

---

<sup>19</sup> Cf. I.1 Considerações sobre a legislação e nota de rodapé 10.

<sup>20</sup> BORGES, Mafalda de Sampaio, *Nótulas para um novo Conceito Estratégico de defesa Nacional – As Informações para o Século XXI*, in Revista Militar n.º 12, Lisboa, Dezembro 2003, pp. 1257-1264.

Segurança e pelas Forças Armadas. Esta demarcação rígida das áreas de intervenção das Forças Armadas e das Forças de Segurança, que foi propósito da lei ordinária, comporta hoje elevados riscos, podendo, no limite, originar vazios de segurança, insuficiências na prontidão requerida e nos mecanismos de resposta necessários, deixando o país manietado perante a materialização de ameaças que actualmente se configuram como as mais prováveis.”<sup>21</sup>

Para se poder efectuar um trabalho de análise de Informações adequado, há que estabelecer uma política de Segurança Nacional que sirva as necessidades de Portugal, pois não se pode processar informação sobre todos os assuntos e não se pode apresentar resultados de Informações sem o decisor político definir claramente o que se pretende. Portugal deve adoptar uma política clara de Segurança e Defesa, estruturada como uma política global do Estado de forma a poder clarificar a análise das ameaças que se nos apresentam e solicitar uma avaliação coerente dessas ameaças. Como contributos para novos conceitos de Segurança e Defesa e com sugestões para a Mudança, apresentamos as considerações do General Valença Pinto por as considerarmos como muito válidas:

“Nova conceptualização e cultura de Segurança e Defesa:

- a. Deixar de assentar a organização da segurança e defesa na ideia de salvaguarda da integridade territorial;
- b. Estruturar a política de defesa na protecção contra riscos difusos, de natureza diversa, manifestados dentro e fora das fronteiras geográficas e, para cuja resposta deve ser sempre possível contar com a eventualidade de emprego efectivo, rápido e decisivo das Forças Armadas;
- c. Considerar que a maior prioridade assenta na capacidade de projectar forças e de as empregar em missões de apoio à política externa, que se torna identicamente estruturadas, se bem que para treino e aprontamento de forças se deva manter como referência a dissuasão e a defesa directa do território;
- d. Atender ao esbatimento das fronteiras entre segurança externa e interna;
- e. Necessidade de activar, utilizar e fazer agir interactivamente todos os recursos (diplomáticos, económicos, militares, culturais, sociais e outros) sob uma direcção política efectiva;

---

<sup>21</sup> Op. Cit. VIANA, 2003, 12.

- f. Considerar que cada Estado Europeu é agora obrigado a ver os seus interesses de segurança e defesa numa nova escala e mais vasta (em comparação com a escala individual do passado);
- g. Aceitar a mudança como regra natural e constante, mas ao mesmo tempo forçando a compaginação desta evidência com a necessidade de ser rápido na formulação das políticas e na adopção de medidas.

Sugestões para a Mudança:

- a. Centrar a política de defesa com as demais políticas do Estado;
- b. Estimular coerentemente uma prática de interligação activa e esclarecida entre os departamentos do Estado com intervenção no domínio da segurança e defesa, em especial entre política externa e a defesa militar;
- c. Capacidade para compreender diferentemente os interesses vitais;
- d. Encontrar uma nova disponibilidade para materializar os empenhamentos;
- e. Promover uma aplicação de recursos que confira eficácia e credibilidade às políticas e aos aparelhos que as servem;
- f. Aplicar judiciosamente os recursos;
- g. Indispensabilidade de existirem políticas activas e empenhadas de contacto e esclarecimento da opinião pública”<sup>22</sup>

Esta síntese do General Valença Pinto vem de encontro ao que será proposto neste trabalho. Um modelo de análise baseado em *data mining* de amplitude global, em que a Segurança Nacional é um todo e as Informações deverão trabalhar de forma a responder oportunamente às solicitações que lhe forem efectuadas.

### **II. 3 Síntese conclusiva**

É consensual que “o ambiente estratégico internacional continua incerto, imprevisível, complexo e perigoso.”<sup>23</sup> Surgem novos actores de matriz incerta, que procuram “o confronto violento com fins escatológicos e de natureza ideológica,”<sup>24</sup> não olhando a meios para atingir os seus fins.

Esta incerteza estratégica acentuou a necessidade de adopção dos conceitos de segurança alargada e de segurança cooperativa; conceitos já introduzidos no CEDN de 2003. Portugal deve conferir uma atenção acrescida a uma filosofia preventiva e atender

---

<sup>22</sup> PINTO, Valença, *Segurança e Defesa*: in Vários, *Estratégia*, nº 16 – 1º Semestre, Instituto de Estudos Estratégicos e Internacionais, 2002, pp. 179-187.

<sup>23</sup> Op. Cit. VIANA, 2003, 2.

<sup>24</sup> Op. Cit. SANTOS, 2003, 80.

a segurança de forma global e, no âmbito das instituições internacionais, empenhando-se no reforço das acções que visem a segurança internacional no quadro da ONU, da Organização para a Segurança e Cooperação na Europa (OSCE) e da NATO, contribuindo para a estabilidade mundial à medida das suas possibilidades.

O Professor Adriano Moreira sublinha que “se verificou uma decisiva desterritorialização da defesa e segurança, muito para além da histórica fixação nas fronteiras geográficas sagradas pelo sangue, uma mudança que pesa na incerteza da época em que vivemos, torna mais exigente a prontidão que assegura a presença cooperativa sem a qual os Estados caminham para exíguos, são dispensados de participar nos centros internacionais de decisão, alienam-se nos factores exógenos, entram em perda de identidade.”<sup>25</sup>

Concluimos que num ambiente tão instável é urgente adoptar, na prática, uma política concertada de prevenção da novas ameaças, colaborar no quadro internacional com Informações próprias e credíveis, conjugando as capacidades de todos os serviços de Informações e das FA e assumindo um conceito de Segurança único.

---

<sup>25</sup> MOREIRA, Adriano et al., *A Defesa Nacional e as Forças Armadas in Estratégia*, Vol. XIV, ed. IPCE, Lisboa, 2003, pp. 14-15.

O objectivo da nossa Política de Segurança é garantir a liberdade e o bem-estar das pessoas – mas também proteger eficazmente a sociedade democrática. Para garantir isto, a simples protecção das fronteiras com meios militares já não é suficiente.

Chanceler Gerhard Schröder<sup>26</sup>

### III – AS AMEAÇAS

#### III. 1 Conceito de ameaça

O trabalho estratégico deve identificar quais os objectivos que se pretendem atingir, quais as ameaças que se perfilam e quais os meios disponíveis, para depois escolher a modalidade de acção estratégica que melhor permita atingir os objectivos delineados.

Além da definição de ameaça, que se encontra no corpo de conceitos, o General Cabral Couto explica que esta é sempre “o produto de uma possibilidade por uma intenção,”<sup>27</sup> em que cada oponente tenta explorar vulnerabilidades do adversário.

Ao longo dos tempos a análise das possibilidades ou do potencial do inimigo foi sendo, normalmente, não muito difícil. Baseava-se em dados materiais e mensuráveis do seu potencial estratégico que eram relativamente fáceis de conhecer. Por vezes, eram mesmo publicitados de forma a desencorajar o adversário. Porém, com as alterações da situação internacional e a emergência de actores desterritorializados, o conhecimento das possibilidades do inimigo torna-se muito mais incerto. Há uma grande dificuldade em conhecer o armamento de que as redes terroristas dispõem, pois a sua aquisição é efectuada ilegalmente. Por outro lado, estes grupos não se coíbem de usar meios não militares como arma e causar danos devastadores, ao nível moral e material.

As intenções destes actores são de natureza subjectiva, o que torna a análise das mesmas muito complexa. Dependem da determinação do adversário, das suas forças morais, e de factores de ordem histórica, sociológica, religiosa e política, podendo, por vezes, assumir rasgos de irracionalidade, como o caso de ataques a escolas matando centenas de crianças. Assim, tanto a análise das suas possibilidades como das suas intenções é ainda mais difícil de efectuar.

As vulnerabilidades da nossa unidade política são conhecidas e devem ser mantidas em segredo e colmatadas o mais breve possível. Conhecer as do adversário é

---

<sup>26</sup> Discurso proferido em Berlim, a 19 de Março de 2004, in KRAFT, TCor Uwe, *A Análise da Política de Segurança e defesa da Alemanha*, CEM, 2003/004, documento policopiado.

<sup>27</sup> Op. Cit. COUTO, 1998, 329

mais difícil, mas devem ser exploradas com brevidade, assim que forem conhecidas pelo decisor político.

Depois de se identificarem as ameaças que se apresentam ao actor político estas devem ser cuidadosa e adequadamente caracterizadas. No entender do General Cabral Couto, os factores que caracterizam as ameaças são: a sua natureza, a sua grandeza ou intensidade, a probabilidade, a durabilidade ou permanência e a sua periculosidade.<sup>28</sup>

### **III. 2 Velhas e novas ameaças**

Pedindo emprestado o título desta secção ao General Loureiro dos Santos, vamos rever o que diversos autores e políticos definem como as ameaças que se apresentam aos países democráticos para, na secção seguinte, analisarmos o CEDN e vermos quais as ameaças consideradas relevantes por Portugal. No apêndice 2, encontra-se uma matriz de comparação com as ameaças identificadas por diversos autores.

#### **III. 2. 1 Velhas ameaças**

O General Loureiro dos Santos chama velhas ameaças ou “ameaças clausewitzianas” às ameaças tradicionais, aquelas que se apresentam como de Estados contra Estados e “que se encontram registadas na história como as principais origens de conflitos”.<sup>29</sup> A origem destas ameaças situa-se nos Estados visando a disputa territorial, de natureza histórica ou étnica, disputando recursos ou a imposição de valores. Foram a origem dos conflitos ao longo da História principalmente durante as ordens mundiais que se seguiram a Westefália. A existência de conflitos decorrentes destas ameaças não impossibilitou a emergência de outras formas de combate e de ameaça, que não o conflito entre Estados.

Desde sempre as técnicas de guerrilha, de terrorismo e de combate pela doença foram adoptadas pelos beligerantes. A resistência à ocupação Romana da península Ibérica, por parte de Viriato, faz-se usando a guerrilha e a sua morte efectua-se subornando os seus lugares tenentes. A contaminação de poços de água nos cercos da Idade Média, para combater os sitiados, era efectuada sempre que possível. O terrorismo selectivo foi usado pelo Exército Republicano Irlandês (IRA) e pelo grupo separatista Basco (ETA),<sup>30</sup> com vista à consecução dos seus objectivos. Apesar de tudo,

---

<sup>28</sup> Op. Cit., COUTO, 1998, 330.

<sup>29</sup> SANTOS, José Alberto Loureiro dos, *Convulsões: Ano III da «Guerra» ao terrorismo – Reflexões sobre Estratégia IV*, Mem Martins, Ed. Publicações Europa-América, 2004, p. 198.

<sup>30</sup> ETA é o acrónimo de *Euskadi Ta Askatasuna* (Pátria Basca e Liberdade).

estas formas de luta estavam limitadas à procura de soluções para uma causa conhecida. Evitava-se o recurso a estas técnicas sem que se pudesse invocar uma racionalidade.

A situação alterou-se radicalmente com o fim da guerra fria. As ameaças de invasão de territórios são de probabilidade baixa e a possibilidade de emprego das FA nessa situação é também baixa.<sup>31</sup> O almirante Reis Rodrigues refere que “no âmbito da NATO, é consensualmente considerada como muito remota a possibilidade de os países membros poderem, no actual contexto de segurança, ficar sujeitos a situações clássicas de invasão territorial.”<sup>32</sup> No entanto, o General Loureiro dos Santos refere que surgem novas ameaças ao nível estatal nas áreas económicas, culturais, mediáticas, de política externa e que não requerem resposta militar.<sup>33</sup>

### III. 2. 2 Novas ameaças

As novas ameaças que se apresentam, chamadas por muitos autores ameaças assimétricas, resultam da situação complexa em que o mundo vive. Após o desmoronamento da ordem imposta pela guerra fria assistiu-se à invasão do Kuwait, à desagregação da Jugoslávia, ao aparecimento dos «estados falhados», ao surgimento de ataques terroristas de dimensão trágica e sem racionalidade aparente. Os ataques de Nova York, Madrid, Bali ou, mais recentemente, de Beslan mostram o horror de que os terroristas sem rosto são capazes por causas, muitas vezes, desconhecidas ou irracionais.

O ambiente estratégico que o mundo vive caracteriza-se pelo facto das “ameaças, antes latentes, serem hoje bem reais, principalmente o terrorismo internacional e a proliferação de armas de destruição maciça. Elas são dirigidas contra os nossos concidadãos, contra os nossos valores, contra os nossos interesses, contra as nossas instituições democráticas.”<sup>34</sup> Esta afirmação do primeiro-ministro francês, Raffarin, reflecte a preocupação da França, a par dos EUA e de outras potências europeias, sobre a necessidade de combater as novas ameaças. As ameaças assimétricas usam métodos e meios não convencionais, que têm por objectivo circunscrever ou destruir as forças materiais e morais de um adversário, explorando as todas as suas vulnerabilidades e fraquezas, incluindo as não militares, provocando efeitos potencialmente desproporcionais.

---

<sup>31</sup> Esta apreciação é concorrente em diversos autores. A avaliação das ameaças, ainda que de forma expedita, é efectuada para se poderem criar cenários de emprego das FA.

<sup>32</sup> RODRIGUES, Alexandre Reis, *Nos meandros da política de defesa*, Editorial Notícias, Lisboa, 2002, p. 38.

<sup>33</sup> Cf. Op. Cit., Santos 2004, pp. 127 e 128

<sup>34</sup> RAFFARIN, Jean-Pierre, *La politique de défense de la France*, in Défense Nationale, Paris, Novembro 2002, p. 5 – Tradução do autor.

O general Loureiro dos Santos considera que as novas ameaças são concretizadas por actores não clausewitzianos de natureza criminosa ou política. Os primeiros actores pretendem obter o máximo lucro sem quaisquer escrúpulos, usando o crime organizado, o tráfico de drogas e de pessoas e a corrupção estatal para atingir os seus fins. Por vezes, podem-se confundir com o Estado, mas não pretendem assumir o controlo e direcção político do Estado. Pretendem controlar o Estado na sombra, colocando políticos corruptos na sua chefia. “Os segundos actores são clara e abertamente natureza política, embora se dissimulem sob outras capas, nomeadamente as étnicas e religiosas, e lançam mão, se o considerarem útil, de todas as actividades criminosas. Visam obter o poder político nacional ou global”.<sup>35</sup>

Notemos que estes actores trabalham muitas vezes em simbiose. Os que têm fins políticos usam os que têm fins económicos para obter fundos e estes usam técnicas de terror para multiplicar os seus fundos. São actores desterritorializados, organizados em redes, cada vez mais complexas e autónomas, difíceis de eliminar, pois sem grande relação hierárquica.

Fruto dos acontecimentos, o terrorismo internacional aparece como a principal ameaça, que os Estados democráticos poderão ter que enfrentar. A par desta ameaça, a proliferação de armas de destruição maciça, (ADM), a que estes grupos poderão vir a ter acesso, constitui uma preocupação permanente. Tais aspectos, associados à chamada revolução da informação, que permite o fluxo de dados e de capitais sem qualquer controlo governamental, expõem todos os países, principalmente aqueles com economias em fase de consolidação, a grandes riscos.

Por outro lado, surgem também ameaças e riscos que não se prendem com a ambição de grupos ou de actores emergentes, mas com a dificuldade de organização social a que se tem assistido nas últimas décadas. A mundialização, o crescimento populacional, a concentração das megalópolis e desintegração social e étnica, a predominância do modelo de mercado e a ameaça do fundamentalismo de mercado, os acidentes ecológicos, as grandes tensões económicas, as especulações financeiras são algumas das novas ameaças ou riscos que o General Loureiro dos Santos considera serem importantes, devendo ser observados no âmbito das diferentes políticas de segurança e defesa.<sup>36</sup> Alguns autores têm considerado o clima como uma das maiores

---

<sup>35</sup> Op. Cit., SANTOS, 2004, 201.

<sup>36</sup> Cf. SANTOS, José Alberto Loureiro dos, *Reflexões sobre Estratégia – Temas de Segurança e defesa*, Mem Martins, Ed. IAEM e Publicações Europa-América, 2000, pp. 38 e 39.

ameaças ao nosso modo de vida. Como esta ameaça é analisada por outros sistemas que não o *data mining*, apresentamos no Anexo A um artigo do jornal britânico, *The Observer*, afirmando a existência de um relatório secreto do Pentágono informando o Presidente dos EUA da grande ameaça que constituem as alterações climáticas previstas para os próximos 20 anos.

### **III. 3 O CEDN e as ameaças externas a Portugal**

Por imperativo de lei, as FA em Portugal só podem actuar contra qualquer agressão ou ameaça externas.<sup>37</sup> Depois de identificadas as ameaças no ambiente estratégico em que vivemos importa analisar o CEDN para identificar quais as ameaças consideradas externas e, por conseguinte, deduzir o CEM e as missões específicas da FA para fazer face a estas ameaças ou agressões. O CEDN foi aprovado em 2003 de forma a reflectir as alterações ocorridas no cenário internacional e os consequentes desafios que são colocados aos actores para “repensar e adequar os conceitos e os instrumentos de segurança e defesa ao novo ambiente político estratégico”.<sup>38</sup>

No capítulo anterior dissertámos sobre a diferenças entre segurança interna e segurança externa, tendo chegado à conclusão, de acordo com os diversos especialistas na matéria, que estas diferenças são, cada vez mais, ténues e que o Estado deve fazer um esforço colectivo ao nível das diversas políticas sectoriais de forma a implementar uma política global coordenada de Segurança e Defesa.

Neste novo cenário de fronteira difusa o governo, através do CEDN, define quais as ameaças e agressões externas que deverão ser consideradas de forma a permitir que as Forças Armadas possam actuar activamente na sua prevenção e combate.<sup>39</sup>

O CEDN no seu capítulo 6, intitulado “As ameaças relevantes”, define como ameaça externa e, quando concretizada, como uma agressão externa, inserindo-se claramente na missão das FA os seguintes aspectos:<sup>40</sup>

- Agressão armada ao seu território, à sua população, às suas FA ou ao seu património;
- Terrorismo transnacional nas suas variadas formas;<sup>41</sup>

---

<sup>37</sup> Cf. LDNFA, art.º 1 e art.º 24 e cf. considerações sobre a CRP I.1 na p. 17.

<sup>38</sup> CEDN, p. 3

<sup>39</sup> Cf. nota 11 na p. 17.

<sup>40</sup> CEDN, p. 12

<sup>41</sup> O CEDN espelha o terrorismo como a mais grave e provável ameaça ao Estado Português. Não estando escrito em letra de forma, as repetidas preocupações com este fenómeno levam-nos a fazer esta dedução, que está de acordo com todos os especialistas consultados.

- O desenvolvimento e proliferação não reguladas de armas de destruição maciça de natureza nuclear, radiológica, biológica ou química;
- O crime organizado transnacional, em especial o tráfico de droga e as redes de promoção e exploração da imigração ilegal e do tráfico de pessoas.
- Os atentados ao ecossistema, incluindo a poluição marítima, a utilização abusiva dos recursos marinhos nas águas sob a nossa responsabilidade e a destruição florestal.

### **III. 4 Síntese conclusiva**

Do que foi referido podemos concluir que as ameaças são um produto da vontade e da força moral do adversário. Se antes existiam ameaças ditas tradicionais em que a sua materialização em agressão só era efectuada se existisse uma possibilidade real de obter a vitória, actualmente entramos numa era de assimetria, de conflitos assimétricos, em que o terrorismo usa meios de luta não convencional, explora as vulnerabilidades das sociedades desenvolvidas e o seu modo de vida.

O desanuviamento na tensão leste-oeste não trouxe uma paz perpétua, antes despoletou um conjunto de tensões regionais e de ideologias fundamentalistas que se encontravam adormecidas.

Os ataques terroristas aos EUA deixaram o mundo perplexo. A sensação que prevalece, hoje, é de insegurança e vulnerabilidade, podemos dizer de impotência. O terrorismo já há algum tempo vinha sendo apontado como uma das principais ameaças à segurança. Não nos basta, apenas, saber que ele existe. O difícil, penoso, angustiante, é saber como, quando e onde ele se manifestará de forma concreta e objectiva. Um ensinamento essencial da actuação dos terroristas é que as fronteiras de segurança não coincidem mais com as fronteiras geográficas dos Estados. Essa fronteira encontra-se em todo o lado em que se manifesta a ameaça terrorista.

Portugal adoptou um CEDN que inventaria, de forma explícita, quais as ameaças que considera externas, portanto aquelas para as quais as FA se devem preparar para enfrentar, caso se concretizem, e que devem ser objecto de uma análise de Informações para as evitar ou, no pelo menos, minimizar. O terrorismo transnacional assume uma importância destacada, pelas numerosas referências que lhe são efectuadas, pelo que consideramos como a ameaça mais premente e que se insere claramente nas missões das FA.

“Em todos os tempos, os estadistas quiseram saber a hora exacta do começo de um conflito, ou seja, ambicionaram vogar acima do tempo, e prever o futuro.”<sup>42</sup>

## IV – O PAPEL DAS INFORMAÇÕES

### IV. 1 Informações e poder do Estado

Ao longo de todos os tempos o homem usou o segredo e a obtenção de informação acerca do objecto ambicionado para conseguir vantagem nos seus negócios. Também os Estados usam o segredo e a procura de informação dos segredos alheios para poderem negociar com superioridade. Torna-se um dos objectivos privilegiados do Estado conhecer os segredos do outro enquanto protege os seus segredos.

Os serviços especializados em obterem informação começaram, sobretudo, no campo militar, sendo os textos mais antigos, sobre o assunto, os do Livro do Êxodo – onde Moisés manda espiões verificar o território de Canaã e os seus habitantes antes de tentar conquistar o território. Se naquele tempo o serviço de meia dúzia de homens colocava Moisés numa situação de poder face ao adversário, facilmente podemos imaginar a dimensão do poder que hoje representam esses Serviços, para os quais trabalham milhares de pessoas apoiadas pela mais moderna tecnologia. As Informações são uma fonte de poder do Estado.

Em português a palavra informação pode ter diversos significados. A sua tradução a partir de definições em Inglês poderá originar confusões. Para compreender melhor o significado das Informações como poder do Estado optamos por apresentar a definição de Abram Shulsky e Gary Schmitt: «*Intelligence is concerned with that component of the struggle among nations that deals with information.*»<sup>43</sup>

Tal como nos apresentam os autores, os Serviços de Informação têm uma dupla natureza: por um lado, lidam com a informação que é necessária para os decisores políticos, por outro, estes Serviços são uma parte do conflito entre nações ou com outros “adversários”, tais como grupos terroristas ou crime organizado.

No primeiro ponto salienta-se o facto de que os Serviços de Informações não têm a função de apresentar modalidades de acção ao poder político. Não apresentam várias hipóteses para que se escolha uma. A sua função primordial é apresentar toda a

---

<sup>42</sup> ROGEIRO, Nuno, *Guerra em Paz*, 1ª ed., Lisboa, Hugin Editores, 2003, p. 921.

<sup>43</sup> SHULSKY, Abram N. e SCHMITT, Gary J., *Silent Warfare – Understanding the World of Intelligence*, Ed. Brassey's, 3ª Edição, Washington D.C., 2002, p. 175.

informação disponível e “prever” com, razoabilidade, o futuro. Não é uma função de adivinhação, antes é tentar ligar um conjunto vasto de informação dispersa de forma a aperceber-se das intenções do adversário e apresentar esses cenários aos decisores políticos, cabendo-lhes a responsabilidade das atitudes a tomar com essa Informação.

Do outro ponto ressalta o objecto da análise dos Serviços de Informações. É o poder político que define qual ou quais são os “adversários” e que tem a responsabilidade de orientar os Serviços de Informações, determinando quais as informações que precisa e sobre que “adversário”. Entende-se adversário, como aquele de quem se pretende obter informações, podendo tratar-se de um país, um grupo terrorista, uma organização criminosa ou ainda um indivíduo. Esta noção advém do facto de que, quem tem a informação, a maior parte das vezes, não a quer disponibilizar, isto é, os Serviços de Informações pretendem ter conhecimento das actividades do “adversário” enquanto este protege os seus segredos e efectua acções de decepção, ou seja, há um esforço organizado por parte do “adversário” para desinformar, tornar turvo o entendimento e negar o conhecimento. Há, assim, entre os Serviços de Informação e os seus adversários, o travar de uma “luta” pelo conhecimento.

Podemos concluir que os Serviços de Informação desenvolvem um conjunto de tarefas, onde a aquisição de conhecimento se torna o objectivo primordial para a consecução das suas funções: apoiar a decisão política, favorecer a disposição estratégica do Estado e fornecer indicadores e alertas sobre os “adversários”.

Em síntese citamos o Cor. Carlos Chaves, “As Informações não são pois utilizadas pelas pessoas ou organismos que as produzem, destinam-se a facilitar e a melhorar o processo de decisão que reside em entidades exteriores e democraticamente responsáveis.”<sup>44</sup>

#### **IV. 2 A necessidade de Informações**

Na secção anterior percebemos que os serviços de Informações são um dos elementos do poder do Estado. Cremos que basta esta constatação para admitirmos que nenhum decisor político, pelo menos em consciência, deve abdicar de tal poder. Este instrumento de poder não serve o decisor político enquanto pessoa, deve-o servir na garantia da segurança do Estado. O Dr. Dias Loureiro chega a afirmar que “não há

---

<sup>44</sup> CHAVES, Carlos, *Tendências organizacionais dos Sistemas de Informações militares. Que modelo para o futuro. Articulação com as organizações Internacionais*. TILD, CSCD 2003/2004, IAEM, Lisboa, 2004, p. 5.

segurança sem Informações”,<sup>45</sup> sendo, estas, uma das garantias de o Estado poder cumprir um dos seus objectivos – garantir a Segurança dos cidadãos.

Numa democracia os serviços de Informações recebem poderes extraordinários para proteger as liberdades dos cidadãos. Precisamente por causa desses poderes, tais serviços, bem como as polícias e as Forças Armadas que formam com eles o núcleo coercivo do Estado, são capazes de causar danos a essas mesmas liberdades e às instituições democráticas. Os riscos envolvidos nesse caso são vários. Num extremo está a instrumentalização dos serviços de Informações por parte de um governo contra seus adversários políticos, enquanto no outro extremo está a autonomização dos serviços e sua transformação em centros de poder independentes no sistema político. Por tudo isto, o tema do controlo político sobre as actividades dos serviços de Informações é central. Na secção seguinte iremos verificar como Portugal articula os seus serviços de Informações e como é exercido o controlo destes serviços.

#### **IV. 3 O SIRP**

Na sua essência os serviços de Informações deverão prover o Estado de Informações necessárias, credíveis e em tempo para a tomada de decisão política. A Informação deve ser solicitada pelo poder político, em circunstâncias determinadas por lei própria, e deve ser integrada ao mais alto nível da decisão, não sendo função destes serviços, distinguir entre Informações de carácter externo ou interno.

O enquadramento legal do SIRP que data de 1984, com alterações de 1995 e 96, não espelha as transformações ocorridas na última década do século XX. Foi um serviço concebido 10 anos após o 25 de Abril, ainda com alguns estigmas do anterior regime, e na sequência do atentado de Montechoro e do assalto à embaixada da Turquia, em 1983<sup>46</sup>. Desde a criação deste serviço as tecnologias de informação e comunicação (TIC) tiveram um avanço espantoso, evolução que trouxe novas ameaças, mas, também, novas oportunidades, ainda não enquadradas na lei destes serviços.

A existência em Portugal de dois serviços com missões estanques, como foi apresentado na resenha legislativa, pode ser um constrangimento à partilha de conhecimento dos diversos organismos e pode provocar a divisão de recursos que sempre são escassos. A reorganização dos serviços de Informações deve passar pela

---

<sup>45</sup> SIMÕES, Pedro, *Os Serviços Secretos em Portugal*, 1ª ed., Lisboa, Ed. Prefácio, 2002, p. 59.

<sup>46</sup> Issam Sartawi, representante da OLP nos trabalhos do XVI Congresso da Internacional Socialista (IS) foi assassinado em Montechoro em Abril de 1983. O acto terrorista foi reivindicado pela organização extremista palestiniana de Abu Nidal. A embaixada da Turquia foi assaltada por um comando Arménio, em Julho de 1983, do qual resultaram 7 mortos.

criação de uma autêntica comunidade de Informações, que envolva e comprometa todos os serviços que trabalham nesta área.<sup>47</sup>

Pensamos que o SIRP pode ter limitações no âmbito da partilha de informação e no uso dos bancos de dados, dado que seu uso se encontra fortemente restringido pela lei. Mas seria importante criar rotinas de partilha de Informação, através da criação de uma comunidade de Informação e da partilha, atendendo a verificações eficazes, de bases de dados.

A segunda limitação que se nos apresenta, é a interligação dos bancos de dados do SIEDM e do SIS. É expresso no ponto 3 do artigo 23.º da lei-quadro do SIRP, que os bancos de dados dos dois serviços não se podem interligar. Podendo compreender as razões do legislador, pensamos que deveria existir uma autoridade que tivesse acesso a ambos os bancos de dados e os pudesse correlacionar. Teríamos, assim, um ganho na qualidade e quantidade de pesquisa e análise de informações obtidas por fontes abertas (OSINT), que são de onde procede o maior volume de informações, e um benefício no acesso a dados quando a ameaça se torna mais difusa. Por outras palavras, se os serviços vocacionados para a pesquisa de ameaças externas tiverem Informações sobre grupos terroristas que entretanto entram em Portugal, há muito trabalho de análise que já está feito e não é necessário alocar recursos de outro serviço a efectuar a mesma análise.

Em consonância com o CEDN, o CEM alerta que as novas exigências que se colocam às FA, no âmbito da segurança interna, na projecção de forças para o Espaço Estratégico de Interesse Nacional Conjuntural (EEINC) e no âmbito dos compromissos assumidos por Portugal, revelam a grande importância de colher, tratar e disseminar atempadamente Informações de natureza militar e aprofundar a articulação com os serviços de Informações da República.

O coronel Chaves propõe um novo Serviço de Informações da República, que apresentamos em Anexo B, por considerarmos que cria as sinergias para um melhor funcionamento do SIRP.

#### **IV. 4 Síntese conclusiva**

As Informações são um elemento essencial de poder do Estado, que este deve usar para «combater» o adversário, aqui entendido em sentido lato.<sup>48</sup> Por exemplo, governos de países amigos podem estar a negociar um tratado e, no aspecto da negociação, são

---

<sup>47</sup> Cf. Op. Cit., CHAVES, 2004, 31

<sup>48</sup> Cf. Op. Cit., SHULSKY, 2002, 1

adversários, ambos tentam conquistar o máximo de proveito do tratado em prejuízo do outro país.<sup>49</sup>

Em Portugal essa recolha e tratamento de Informações é feito no âmbito da lei-quadro do SIRP, que ainda não reflecte as profundas transformações no ambiente estratégico internacional e um novo quadro de ameaças que foi apresentado. Um bom Serviço de Informações é de um valor inegável para o Estado Português e a sua estruturação deve poder responder aos novos desenvolvimentos da política internacional e aos desenvolvimentos tecnológicos. Dever-se-à adoptar sistemas de análise de informação que possam ser adaptados a novas exigências, mantendo um controlo rigoroso por parte das entidades competentes.

Já no decorrer deste trabalho, vieram a lume na imprensa, notícias de uma possível reestruturação do SIRP com a possibilidade alterações profundas à lei-quadro.<sup>50</sup> Depois de falarmos com alguns possíveis intervenientes no processo pensamos que as decisões ainda se encontram em fase de estudo e seria prematuro analisar as notícias publicadas.

---

<sup>49</sup> Portugal tem excelentes relações com os países da UE. No entanto, no que diz respeito à política africana, Portugal encontra pontos de vista opostos em alguns dos seus parceiros da UE. Claro que nestes casos a troca de Informações sobre política africana entre países da UE é um assunto melindroso.

<sup>50</sup> FREIRE, Manuel Carlos, *Forças Armadas criam um novo serviço de Informações*, in Diário de Notícias, 20 de Setembro de 2004.

“Information analysis is the brain of homeland security. Used well, it can guide strategic, timely moves throughout our country and around the world. Done poorly, even armies of guards and analysts will be useless.”<sup>51</sup>

## V – MÉTODOS E FACTORES PARA ANÁLISE DAS AMEAÇAS

Depois de identificar as ameaças que se apresentam, o decisor político necessita de conhecer quais as possibilidades de se concretizarem, quais os danos que podem provocar e o que se pode fazer para minimizar esses danos. Esta informação só é útil se for fornecida em tempo oportuno. De facto, se o decisor souber apenas com horas ou minutos de antecedência que vai haver uma invasão do seu território pouco poderá fazer para conter essa invasão. No entanto, no caso de um ataque terrorista esse tempo pode ser crucial. Temos assim que o aviso oportuno depende do tipo de ameaça e da organização que a leve a cabo.

Desde sempre o homem quis prever o futuro, conhecer a acção do seu inimigo para lhe poder fazer face, seja negociando, seja preparando a sua defesa, ou atacando preventivamente. Os serviços de Informações têm acometida a tarefa de antever sobre quais as ameaças que se podem concretizar e qual o seu grau de perigosidade. É uma tarefa de previsão, nem sempre correcta porque além de se basear em factos conhecidos e na história, também se baseia na percepção do analista. É uma tarefa intelectual de inteligência e de estudo de comportamentos que se baseia em indicadores e avisos.

A forma de analisar e avaliar as ameaças tem evoluído ao longo dos tempos e depende fortemente do ambiente estratégico. Neste capítulo iremos tecer algumas considerações sobre indicadores e avisos, as formas tradicionais de avaliação de ameaças e o novo sistema da NATO, o *Nato Intelligence Warning System* (NIWS).

### **V. 1 Conceito de indicadores e avisos**

Os indicadores e avisos nos sistemas de Informações são usados para alertar os decisores políticos do início da crise de forma a estes poderem reagir.

Um aviso, como vimos no corpo de conceitos, prende-se com a tomada de decisões depois de se conhecer a informação disponível. Não é um acontecimento isolado no tempo, antes é um processo cíclico em que uma crise, um risco ou uma ameaça identificáveis são avaliados, dando origem à definição de um problema de alerta

---

<sup>51</sup>BAIRD, Zoë et al., *Protecting America's Freedom in the Information Age*, Markle Foundation, Outubro de 2002, disponível em: [http://www.markletaskforce.org/report1\\_overview.html](http://www.markletaskforce.org/report1_overview.html)

e ao estabelecimento de uma lista de indicadores decisivos. Em seguida, os indicadores decisivos são controlados em permanência e os sistemas de avaliação são actualizados.

Os indicadores sendo acções ou acontecimentos que ajudam a perceber se algum evento prejudicial pode surgir, são elementos de previsão. Consoante a situação vai evoluindo, podem-se criar indicadores decisivos ou cruciais, destinados a serem continuamente monitorizados, por representarem um indício significativo do que se está a passar. Estes devem ser definidos tão cedo quanto possível pois, se observados, transformam-se em indicações claras do estado final de uma série de acontecimentos. Os indicadores cruciais são os acontecimentos que materializam a decisão do analista e podem, ou não, provocar a emissão de um aviso sobre a situação de crise.

Os sistemas de indicadores e avisos pretendem detectar e relatar, em tempo oportuno, acontecimentos que ameacem uma entidade política de forma a permitir a tomada de decisão suportada em factos verificáveis. A implementação deste sistema é tanto mais difícil quanto mais complexo e volátil for o ambiente estratégico.

## **V. 2 Métodos de análise**

Durante os períodos das guerras clausewitzianas a avaliação da ameaça assentava na recolha de informação sobre as capacidades militares do inimigo e na sua determinação em empreender uma guerra. Os indicadores eram baseados na sua capacidade industrial, na indústria de guerra que implementava e na situação política que se vivia. A obtenção de Informações era efectuada por espões, meios diplomáticos, e, quando disponível, por meios tecnológicos avançados como satélites, fotografia aérea, entre outros. A recolha de informação sobre as capacidades militares do inimigo era crucial, era necessário conhecer o seu dispositivo, o número de homens, o seu armamento e a capacidade de produção caso um conflito deflagrasse. Por outro lado, era premente conhecer a situação política que se vivia, sendo esta, muitas vezes, a principal razão da concretização, ou não, da ameaça.<sup>52</sup> Por muito evoluídos que fossem os sistemas de obtenção de informação, aquela que sempre foi a preferida pelos serviços de Informações, foi a possibilidade de obter e decifrar mensagens entre as diversas organizações do adversário. Esta é a melhor forma de conhecer as intenções do inimigo, não sendo isenta de erros, pode também ser uma forma de decepção.

---

<sup>52</sup> Cf. HERMAN, Michael, *Intelligence Power in Peace and War*, 1ª Edição, Cambridge, Ed. Cambridge University Press, 2003, 1996, pp. 82 a 99.

Durante o período da guerra fria, os indicadores eram baseados nos passos que o adversário deveria executar para preparar uma força militar. Eram indicadores mensuráveis, muito baseados em dados militares, embora não exclusivamente, que podiam antecipar qualquer agressão. O trabalho de análise era objectivo e visava recolher indicações suficientes de preparação de uma força militar que pudesse, com sucesso, invadir outro país. Os meios tecnológicos estavam vocacionados para a obtenção de informações sobre o desenvolvimento industrial de novos sistemas de armas, a HUMINT, mais conhecida por espionagem<sup>53</sup>, visava recolher informações sobre os chefes militares e segredos de armamento, se possível roubar alguns sistemas de armas.

O método tradicional de avaliação das ameaças era baseado na sua probabilidade, perigosidade e possibilidade como factores de análise, e assentava em métodos indutivos e dedutivos, fortemente apoiado na experiência do analista, na história conhecida e na capacidade de recolha de informação crítica, efectuada, muitas vezes, de forma clandestina.<sup>54</sup> A análise de informação consistia em efectuar inferências sobre os diversos indicadores observados e sobre as possibilidades do inimigo.

A última década assistiu a transformações profunda na natureza das ameaças provocando, no período inicial, um colapso dos sistemas de Informações dos diferentes países, da NATO e da própria ONU. A NATO sentiu necessidade de criar uma nova metodologia de antecipar crises o NIWS, que vamos abordar de seguida.

### **V. 3 O NIWS**<sup>55</sup>

“Os ensinamentos da última década nos Balcãs e noutros sítios são claros. O alerta precoce de crises iminente é vital. Uma acção rápida – e adequada – é inestimável.”<sup>56</sup> Desta forma o Professor John Kriendler, professor de questões de segurança da NATO, enfatiza a necessidade que a NATO sentiu de criar um sistema de alerta para as ameaças que se lhe deparam e que se veio a concretizar no NIWS.

---

<sup>53</sup> Para alguns autores os conceitos de HUMINT e de espionagem são diferentes. Aqui usamos a pirâmide de HUMINT de Michael Herman por a considerarmos como a mais relevante na sistematização dos conceitos. Cf. HERMAN, 1996, 61 a 66.

<sup>54</sup> Cf. DeROSA, Mary, *Data Mining and Data Analysis for Counterterrorism*, Ed. Center for strategic and International Studies, Washington, D. C., 2004, p. 5. Disponível em [www.csis.org](http://www.csis.org).

<sup>55</sup> Este sistema tem como base o MC 166/2004. Por ter um elevado nível de classificação NATO não iremos apresentar os indicadores por ameaça nem os alvos de avaliação por parte da NATO. Apesar de termos tido acesso ao MC referido iremo-nos apoiar nos documentos disponíveis na Internet e no manual do curso de NIWS que não apresenta classificação de segurança. No entanto não iremos apresentar as matrizes de avaliação por considerarmos que podem conter informação sensível.

<sup>56</sup> KRIENDLER, John, *Anticipating crises*, NATO Review, Inverno de 2002, disponível em <http://www.nato.int/docu/review/2002/issue4/english/art4.html>

O NIWS é um programa, baseado num conjunto de três matrizes, que se apoia em processos analíticos qualitativos, não se baseia apenas na medição mecânica de acontecimentos múltiplos, definidos com precisão e específicos. Como tal, cobre não só ameaças para a NATO, mas também uma grande variedade de indicadores de risco militares e não militares, incluindo a incerteza e a instabilidade na área euro-atlântica e áreas adjacentes, e a possibilidade de crises regionais na periferia da Aliança. Além disso, alerta para quaisquer instabilidades, crises, ameaças, riscos ou preocupações em desenvolvimento susceptíveis de ter impacto nos interesses de segurança da Aliança e controla a redução de intensidade das crises.<sup>57</sup>

O NIWS vai para além do planeamento tradicional de forças dos conflitos entre actores-estado, abordando áreas consideradas não tradicionais como as ameaças assimétricas, transnacionais, terrorismos, ADM e ataques a redes de computadores.

Este sistema tem um conjunto de indicadores para cada tipo de ameaça que é definido, pelo MC 166 *Intelligence Working Group* (IWG), e uma matriz de avaliação da actividade que se procura observar.<sup>58</sup> É estabelecido um conjunto de indicadores decisivos que, se verificados, podem levar a que seja emitido um aviso sobre a natureza da ameaça encontrada. Sempre que um aviso é emitido tem de conter qual o actor, qual a acção que preocupa os interesses da NATO, onde a acção tem lugar e porque é que a acção tem lugar.

Os indicadores de análise estabelecidos abrangem as componentes políticas, militares, económicas, sociais e transnacionais, sendo depois especificados para cada tipo de ameaça. Os factores de análise gerais baseiam-se na capacidade operacional, nas intenções, na actividade e no ambiente operacional sendo, depois, detalhados para cada ameaça, sendo elaboradas três matrizes de análise que se preenchem com os dados recolhidos por cada entidade.

Esta metodologia exige que os analistas decidam antecipadamente que acontecimentos ou indicadores cruciais podem servir para a emissão de um aviso. Aqui os analistas devem apoiar-se, não apenas numa abordagem matemática e quantitativa, mas também numa análise qualitativa e de previsão de forma a fornecer avaliações do desfecho das várias situações.

Este sistema visa obviar os problemas sentidos pelos serviços de Informações após o fim da guerra fria, quando houve um forte desinvestimento na HUMINT e um

---

<sup>57</sup> Cf. Op. Cit. KRIENDLER, 2002, 2.

<sup>58</sup> Sobre a actividade que é desenvolvida não nos é permitido apresentar exemplos. Vide nota 55.

crescendo na TECHINT, por vezes considerada como a melhor e mais fiável fonte de recolha e análise de informações. As crises vividas pela Aliança nos Balcãs vieram revelar que era necessário não descurar o elemento humano, sobretudo na análise de Informações.

Por melhor que seja um sistema de alerta precoce, o seu êxito depende, sobretudo, da apreciação e visão dos decisores políticos. “Em última análise, a vontade política para agir, individual e colectivamente, e para intervir, se necessário, é mais importante que qualquer instrumento de alerta precoce. Contudo, a vontade política depende de mais que de uma simples análise da evolução provável dum conflito e é claramente afectada por um grande número de outras questões, incluindo os ciclos eleitorais, as prioridades internas concorrentes e a opinião pública.”<sup>59</sup>

O NIWS é um mecanismo rigoroso de criação de Informações fiáveis, pois congrega métodos tradicionais com poderosas técnicas computacionais. Por outro lado, é um mecanismo participativo, apoiado numa rede de comunicações segura, para onde todos os países podem, e devem, contribuir.

#### **V. 4 Síntese conclusiva**

Ao longo deste capítulo vimos que a análise de informações é um elemento crucial no processo de produção de Informação.

Para que o decisor político possa tomar uma decisão apoiado em evidências, deve ser estabelecido um conjunto de indicadores cruciais a observar e analisar. Como a história recente tem mostrado, este conjunto de indicadores deve ser analisado de forma qualitativa e quantitativa, pois há percepções que só o analista, fruto da sua experiência, pode ter. O investimento nos meios humanos para recolha e análise de informação é pois crucial. Os métodos de análise tradicionais, vocacionados para a guerra fria, não perderam a actualidade, antes necessitam de ver reformulado o seu conjunto de indicadores. Actualmente os alvos da pesquisa de informação são difíceis de identificar, o que obriga a que os Serviços de Informações tenham um trabalho acrescido na recolha e análise das informações, sendo fundamental a ajuda das TIC.

A NATO e os EUA sentiram essa necessidade e estão a fazer um esforço para inverter a situação que se criou com o fim da guerra fria, em que se acreditou que a tecnologia poderia substituir o HUMINT. A NATO criou o NIWS que serve de modelo

---

<sup>59</sup> Op. Cit., KRIENDLER, 2002, 2.

de aviso de ameaças ou de riscos para a Aliança, tendo, na crise do Kosovo, mostrado ser eficaz.

Em síntese podemos acrescentar, que o analista de informação deve ser apoiado por sistemas tecnológicos avançados sem descurar o elemento humano, como fundamental, sendo tão importante investir em sistemas tecnologicamente avançados, como na formação dos analistas que com eles trabalham.

“For counterterrorism, we must be able to find a few small dots of data<sup>60</sup> in a sea of information and make a picture out of them”

Mary DeRosa<sup>61</sup>

## **VI. UM MÉTODO PROPOSTO: ANÁLISE DE DADOS COM DATA MINING**

Após o que foi referido não só é claro que estamos perante um novo espectro de ameaças muito diferentes daquelas que se apresentaram aos Estados durante quase meio século de guerra fria, como também, na área da obtenção e análise de Informações, é necessário o emprego de novos meios e tecnologias de forma a perceber as novas ameaças e prever as acções de novos actores não estatais, que não se coíbem de utilizar meios não tradicionais.

A análise de uma ameaça a que chamámos velha, assenta na obtenção de Informação sobre a sua capacidade militar e da sua intenção de a empregar. As novas ameaças assentam em reduzidas peças de informação de diversas fontes que terão que se juntar para se fazer uma avaliação válida dessa informação. Uma outra forma de podermos obter a informação será conseguir colocar agentes infiltrados junto das organizações terroristas e de crime organizado. Este aspecto de HUMINT, apesar de ser muito relevante, está fora do âmbito deste trabalho. Concentramo-nos, por isso, na apresentação de novos conceitos de análise de informação e descoberta de conhecimento apoiados em sistemas de *data mining*.

### **VI. 1 Conceito de *Data Mining***

Como foi expresso no corpo de conceitos, *data mining* é o processo de descobrir informações relevantes, como padrões, associações, mudanças, anomalias e estruturas, em grandes quantidades de informações armazenadas em bancos de dados, repositórios de dados ou outros mecanismos de guarda automática de informação. É um mecanismo de transformação de dados de baixo nível em informação de alto nível, ajudando no processo de tomada de decisão através do uso de algoritmos de exploração de grandes quantidades de dados de forma a descobrir novos padrões e relações, ou ainda a comparar com padrões conhecidos.

Em suma, o *data mining* é um conjunto de procedimentos para extracção de padrões a partir de bancos de dados e insere-se no processo global de descobrimento de

---

<sup>60</sup> A terminologia inglesa adoptou a expressão «*connecting the dots*», unir os pontos, para classificar a obtenção de Informações referentes às novas ameaças. Esta expressão é uma analogia com os passatempos infantis em que unindo pontos numerados se obtém uma imagem com significado.

<sup>61</sup> DeROSA, 2004, 5.

conhecimento útil em bases de dados, KDD (*Knowledge Discovery in Databases*). O KDD é a base de um sistema de informação inteligente. Compõe-se de um conjunto de passos a serem executados sobre uma, ou mais, base de dados inicial com o objectivo de extrair os conhecimentos desejados que possam estar contidos nessas bases de dados. O *data mining* é a parte principal do processo de KDD.<sup>62</sup>

A análise de grandes volumes de informação não é nova. Tem sido usada pelo sector privado para a obtenção de informações e padrões de comportamento de clientes e pelo sector público na área da fraude e evasão fiscal. Em Espanha o projecto ZUJAR<sup>63</sup> aplica técnicas de *data mining* para detecção de evasão e fraude fiscal, a aplicação CORAL<sup>64</sup> usa estas técnicas para descobrir sistemas de lavagem de dinheiro, o Projecto ECHELON<sup>65</sup> usa-as para analisar comunicações ao nível mundial, o governo dos EUA utiliza *data mining* para identificar padrões de transferências de fundos internacionais que se assemelhem a lavagem de dinheiro do narcotráfico.

As técnicas de análise automática de dados ou de procura de padrões não substituem o analista de Informações, mas ajudam a libertá-lo de tarefas mecânicas de explorar grandes volumes de informação, para que ele se possa dedicar a assuntos que requeiram o seu julgamento. Estas técnicas também ajudam a priorizar a informação mais relevante, e a eliminar aquela sem significado para o analista.

### **VI. 1. 1 Análise por assuntos ou ligações**

A análise de grandes volumes de informação é efectuada, tradicionalmente através de assuntos ou análise de ligações. Ou seja, quando um analista pretende conhecer as actividades de determinado indivíduo começa por procurar o seu cadastro, o seu registo criminal, as transacções bancárias que realiza, as deslocações e as pessoas com quem está ou esteve em contacto. Para cada informação que vá recolhendo pode, depois, ir acrescentando mais um elo numa cadeia de ligações que vai efectuando. Pode até ser

---

<sup>62</sup> Cf. GONÇALVES, Rodrigo e Hillesheim, *Sistemas de Informação inteligentes*, UFSC, Santa Catarina, 2003, disponível em [www.inf.ufsc.br/~rodrigog/free/TranspIA.pdf](http://www.inf.ufsc.br/~rodrigog/free/TranspIA.pdf).

<sup>63</sup> ZUJAR; este projecto da administração tributária de Espanha está a ser implementado usando sistemas de *data warehouse* e *data mining*. Pretende-se encontrar todos os contribuintes que tenham padrões de comportamentos iguais aos que fogem ao pagamento de impostos. Informações mais detalhadas podem ser encontradas em: <http://www.dgci.min-financas.pt/ciat/DocsTecnicos/espanhol/1espana.doc>.

<sup>64</sup> CORAL; *Money Laundry Pattern Learning and Detection Using Data Mining Techniques*, A aplicação tem uma versão de demonstração na Internet: <http://www.fortune.binghamton.edu/demo/CoralDemo.html>

<sup>65</sup> ECHELON; o mais mediático e contestado programa dos EUA na área de escutas telefónicas, análise de correio electrónico e quaisquer telecomunicações. Estas escutas ocorrem em todo o mundo e usam técnicas de *data mining* para seleccionar as comunicações que devem ser alvo de escutas permanentes.

ajudado por software poderoso, tipo «i2»<sup>66</sup>, que permite correlacionar factos e a descobrir ligações imperceptíveis à primeira vista. Esta é a actividade normal e mais usada pelos investigadores, quer no âmbito das polícias, quer no âmbito dos serviços de Informações. Ou seja, para se começar a obter e analisar informação sobre uma actividade ou uma pessoa começa-se por interrogar as bases de dados com o assunto ou nome da pessoa em questão. Por vezes, é possível também obter informação de outras actividades ilícitas praticadas por pessoas ou por organizações através do conjunto de ligações que vão sendo estabelecidas. Uma análise de ligações poderá ser efectuada com vários graus de separação e, assim, obter um conjunto de Informação que possa impedir que a ameaça que estamos a analisar se concretize.

Uma análise dos ataques de 11 de Setembro, efectuada pela *Markle Foundation Task Force*, mostra como é possível extrair ligações complexas e obter informação relevante sobre os planos dos terroristas. Se tivesse sido possível integrar, ao mais alto nível, toda a informação disponível, tais como listas de pessoas sob suspeita, registos de reservas de voos, e dados de residências entre outros, os terroristas poderiam ter sido identificados a tempo de se poder iniciar uma investigação. No apêndice 3 apresentamos uma adaptação do resultado dessa análise efectuada por Mary DeRosa e Zoë Baird.

## **VI. 1. 2 Análise de padrões**

A análise de padrões é menos objectiva e de efectuação mais complexa. Não se procura um suspeito, mas procurar-se encontrar padrões de comportamento, que se conheçam como ilícitos, e depois encontrar quem actua segundo esses padrões. Ao contrário da pesquisa por assuntos, a pesquisa por padrões não necessita de uma pista inicial. Apenas se necessita de conhecer um padrão de actividade ilegal.

Pesquisas baseadas em padrões podem servir para investigar, sistemas conhecidos de lavagem de dinheiro, actividade terrorista adormecida, crime organizado, tráfico de seres humanos e narcotráfico. Por exemplo, se uma rede de lavagem de dinheiro com ligações a uma rede terrorista for identificada, descobrindo o padrão de actuação, pode-se tentar encontrar o mesmo padrão numa base de dados. Se o padrão for encontrado teremos que prosseguir as investigações reduzindo o universo de possíveis suspeitos. À medida que o processo for evoluindo podemos chegar a um conjunto de suspeitos que

---

<sup>66</sup> i2; Software usado para encontrar relações entre pessoas, organizações ou factos com apresentação de forma tridimensional, que seriam muito difíceis de encontrar com os métodos de análise tradicionais. É usado pelos serviços de Informações e pela investigação criminal. Em Portugal o BISM tem usado, experimentalmente, este software, com resultados excelentes. Uma demonstração pode ser vista em [www.i2.co.uk](http://www.i2.co.uk).

poderão ficar sob vigilância para se aferir da actividade criminosa ou não. O mesmo se passa com a análise de tráfego na Internet ou de actividades terroristas. Se procuramos terroristas que possam efectuar um ataque com camiões carregados de explosivos, podemos analisar o aluguer de camiões, em conjunto com a aquisição de explosivos para actividades legais e o alojamento em hotéis e a recepção de mensagens de correio electrónico ou correio suspeito. Padrões de envio de correio electrónico, de conversas telefónicas, números de contas, hotéis registados e pagos em dinheiro, podem indicar onde se encontram os líderes e como enviam mensagens para os seus operacionais.

Estas ferramentas de análise são largamente usadas no meio comercial para obtenção de padrões de consumo, promovendo produtos que se prevê ter interesse para o cliente. Em Portugal, as cadeias de supermercados com cartão de cliente são as que mais usam estas técnicas, algumas instituições bancárias empregam-nas para a concessão de crédito, e as redes internacionais de vendas pela Internet usam-nas para aumentar os lucros e fidelizar clientes.<sup>67</sup>

Como veremos, no capítulo seguinte, é necessário termos um padrão de comportamento para podermos detectar outros. Este padrão ou é conhecido de grupos que já o usaram ou pode ser inferido, sendo, neste caso, a possibilidade de erro muito maior.

## **VI. 2 O Processo**

Na figura seguinte apresenta-se o processo de extracção de conhecimento a partir de bases de dados. Vamos apresentar o que consideramos como importante conhecer para permitir a tomada de decisão de emprego deste sistema.

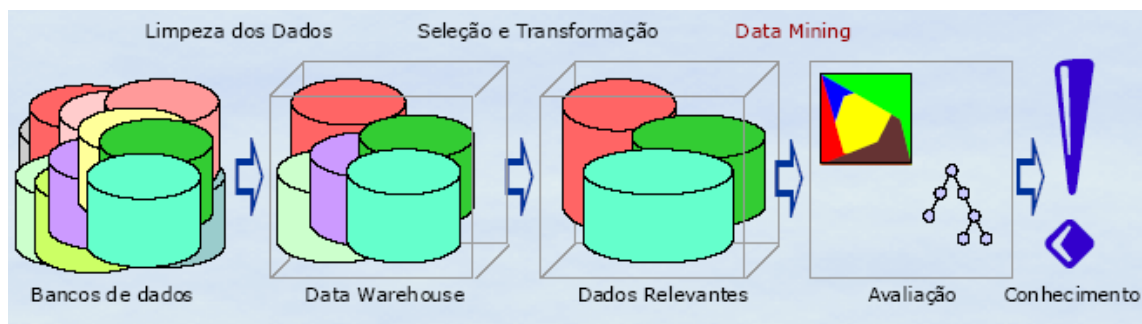


Fig 1 – Processo de extracção de conhecimento

(fonte: [www.lac.inpe.br/eventos/downloads/data.pdf](http://www.lac.inpe.br/eventos/downloads/data.pdf))

<sup>67</sup> Isto pode ser verificado na aquisição de livros na Amazon.com. Sempre que o cliente adquire um livro é-lhe proposto a aquisição de outros títulos, informando, claramente que quem compra determinado livro “costuma” comprar os títulos propostos.

## VI. 2. 1 Recolha e processamento de dados

O primeiro passo consiste em identificar, recolher e processar os dados que, posteriormente, serão analisados. Este é uma etapa fulcral do sistema, pois pode tornar o sistema insignificante se não tiver os dados correctos ou se o “lixo” for tanto que torna inoperacional o funcionamento da pesquisa. A eliminação de registos errados de uma base de dados é uma tarefa muito complexa.

Os dados seleccionados na etapa anterior são então combinados numa base de dados chamada de *data Warehouse*, para depois ser pesquisada. Esta *data warehouse* pode ser física ou virtual. No primeiro caso a informação é recolhida a partir dos vários organismos que se encontram legalmente possibilitados para recolher a informação criando-se uma base de dados centralizada. No segundo caso apenas é estabelecido um conjunto de ligações que permitam a criação de bases de dados distribuídas. Nas bases de dados centralizadas temos a vantagem da facilidade de análise da informação e como desvantagem a manutenção e actualização dos dados. Nas bases de dados distribuídas acontece o contrário.

Apesar de esta ser a forma mais eficaz de trabalhar, se existirem constrangimentos legais ou de acesso podemos aplicar uma análise de padrões sobre uma base de dados tal como se encontra. Se for necessário garantir a privacidade no uso da informação poder-se-á criar uma arquitectura distribuída que permita diferentes acessos e normas de aplicação diferentes consoante se for encontrando transacções suspeitas. Este processo dificulta o uso da base de dados para outros fins que não os previstos inicialmente.

O passo seguinte consiste na transformação e normalização de dados. Este tratamento de informação é fundamental para se poder obter um conjunto de dados relevantes. Por exemplo, numa base de dados os nomes podem estar completos ou abreviados. Tó Zé pode significar António José ou Luís pode ser nome próprio ou apelido. Também as moradas são escritas de diversas formas. Há a Rua da Liberdade e a Avenida da Liberdade, R/C D pode significar Rés-do-chão direito ou fracção D. Em todas as bases de dados, e porque não há normalização entre entidades, eventualmente poderá existir dentro de uma entidade<sup>68</sup>, há diferentes formas de representar a

---

<sup>68</sup> Mesmo em entidades onde há normas difundidas para a recolha de informação em bases de dados os erros são comuns. Os sistemas mais fiáveis são aqueles que obrigam o utilizador a escolher uma opção e que implementam códigos de segurança nos números identificadores. Um exemplo acontece com o número de contribuinte em que o último algarismo é um código de segurança que impossibilita o operador de registo de dados de digitar mal o número.

informação. Ou seja, a informação deverá ser tratada para se poder ter dados relevantes e se aplicar o processo de *data mining*.

## VI. 2. 2 Modelos de pesquisa

Como foi referido, na análise de padrões é necessário a criação de um modelo que se possa aplicar aos dados. De uma forma genérica há dois processos ou métodos de *data mining*: de cima para baixo (*top-down*) ou de baixo para cima (*bottom-up*)<sup>69</sup>.

A abordagem de cima para baixo começa com uma hipótese e procura validá-la. A hipótese pode ser elaborada tendo, inicialmente, pesquisado os dados usando a técnica de baixo para cima ou desenvolvida com conhecimento de um padrão real. A experiência ou dados dos serviços de Informações podem, e devem, ser a fonte destas hipóteses que serão aplicados aos dados. A determinação desta hipótese ou padrão é um trabalho que exige pessoal muito especializado e treinado.

O método de baixo para cima analisa os dados e extrai padrões ou anomalias que indiquem certo comportamento. Este método pode ser directo ou supervisionado (quando se tem alguma ideia do que se pretende encontrar) ou indirecto ou não supervisionado (quando não se tem ideia do que se procura).<sup>70</sup> Este método cria, a partir de um grupo, a identificação de um subgrupo de pessoas que usam um determinado padrão que depois será validado por fontes de Informação tradicionais.<sup>71</sup>

Os sistemas de *data mining* só poderão gerar conhecimento válido se o modelo for válido. Como os padrões que se procuram dizem, normalmente, respeito a pessoas que usam métodos evasivos, que tentam esconder e apagar todo o rasto das suas actividades quotidianas, a possibilidade de existência de falhas na pesquisa de informação é muito grande. Daí a necessidade de poder avaliar toda a informação disponível ao mais alto nível. Dada a exiguidade de informação e o “ruído” que esta possa ter, todos os aspectos são relevantes. Os EUA usam este sistema no programa, *Terrorism Information Awareness* (TIA) da *Defense Advanced Research Projects Agency* (DARPA) que engloba todas as fontes de dados do governo dos EUA. Este projecto baseia-se na pesquisa de informação através de *data mining*. Na ideia de John

---

<sup>69</sup> Apresentamos a terminologia inglesa porque é recorrente o seu emprego, nas obras escritas em português.

<sup>70</sup> Op. Cit., TAIPALE, 2003, 30.

<sup>71</sup> A esta técnica chama-se de “*clustering*”, agrupamento. São criados grupos de padrão comportamental perfeitamente definidos e conhecidos. Os novos dados são colocados na matriz de avaliação e é calculada a menor distância a cada grupo. O novo registo é então associado a esse grupo e determinada a margem de erro. Esta técnica é usada pelas instituições bancárias para a concessão de crédito e negociação da taxa de juro. Cf. Op. Cit. TAIPALE, 2003, 29 e ss.

Poindexter, director do projecto TIA, os “EUA tornam-se assim, muito mais eficientes na pesquisa e geração de informação tornando-a disponível para análise, convertendo-a em conhecimento para fazer face a novas ameaças. Os EUA devem partilhar informação entre todas as agências e criar equipas de apoio de elevado desempenho operando nas margens das organizações terroristas”.<sup>72</sup> Outro projecto adoptado pelos EUA, usando sistemas de *data mining*, é o *Computer Assisted Passenger Pre-Screening* (CAPPS II), desenvolvido pela Agência de Segurança de Transportes após o 11 de Setembro. Na efectivação de uma reserva de um voo, o CAPPS II tem como objectivo fornecer à Agência de Segurança de Transportes, o nome do passageiro a sua morada, data de nascimento e o número de telefone de contacto o que permite efectuar uma verificação da identidade do passageiro e uma avaliação de risco de terrorismo.<sup>73</sup>

Estes sistemas estão implementados e a funcionar. São uma forma poderosa de avaliação da ameaça com tempo muito reduzido. Porém, como veremos na secção 3 deste capítulo, a utilização destes sistemas nem sempre é consensual, podem ser utilizados como uma forte ameaça às liberdades e privacidade dos cidadãos. Nos EUA há uma grande controvérsia com estes projectos tendo sido, por várias vezes, postos em causa pelo Congresso.<sup>74</sup>

## VI. 2. 3 Avaliação e tomada de decisão

O processo de aplicação de técnicas de KDD a um conjunto de bases de dados termina com a avaliação dos resultados obtidos e com as decisões que poderão ter que ser tomadas sobre o emprego dos resultados. No contexto das políticas dos Serviços de Informações existem um conjunto de restrições de ordem legal que não podem ser omitidos. Apesar de nas organizações comerciais se usarem técnicas de análise de padrões de forma automática, nos serviços governamentais o seu emprego deve ser parcimonioso. Estas ferramentas deverão destinar-se à obtenção de informação inicial que será depois confirmada, ou não, pelos analistas de Informações. A avaliação dos

---

<sup>72</sup> POINDEXTER, John, *Overview of the Information awareness Office*, Conferência DARPA Tech, Agosto de 2002, p. 1. Disponível em [www.darpa.mil](http://www.darpa.mil). Este projecto começou por ser conhecido como *Total Information Awareness*. Este programa foi cancelado pelo Congresso dos EUA, em finais de 2002, e obrigado a ser integrado nos projectos da DARPA de forma a evitar a possibilidade de abusos sobre as liberdades dos cidadãos. Este programa continua a ser desenvolvido, em moldes relativamente diferentes, nos programas do Information Awareness Office (IAO) da DARPA. Cf. Op. Cit. TAIPALE, 2003, 19 e [www.darpa.mil](http://www.darpa.mil).

<sup>73</sup> Cf. [www.tsa.gov](http://www.tsa.gov); sítio oficial da Agência de Segurança de Transportes.

<sup>74</sup> Estes são alguns dos sites, entre muitos, em que se apresentam objecções a este programa: <http://www.nytimes.com/2002/11/14/opinion/14SAFI.html>, <http://www.epic.org/privacy/profiling/tia/>, <http://www.unknownnews.net/031001a-nt.html>.

resultados finais deverá ser sempre da responsabilidade de uma pessoa certificada para aceder a informação delicada.

No patamar de tomada de decisão dever-se-á ter em consideração os aspectos legais de uso da Informação, possibilidade de comunicação a outras forças policiais ou judiciais e ainda a possibilidade de extravio dessa Informação. Isto é muito relevante quando se procuram padrões muito difíceis de provar, junto do poder judicial, antes de a acção acontecer. Por exemplo, se procurarmos padrões de lavagem de dinheiro e obtivermos sucesso, em teoria será possível descobrir a pessoa que a efectuou e accionar os mecanismos legais necessários. No caso de evitar um atentado terrorista o problema é muito maior. De facto, antes de o atentado se perpetrar estamos no campo das intenções. Estas ferramentas podem detectar um padrão de comportamento que se conhece como o tido pelos terroristas e não ser terrorista. É difícil provar que uma pessoa tem em mente a execução de atentado terrorista se não existirem provas materiais, com planos, explosivos, mensagens, que o suportem.

A avaliação e uso de Informação obtida por meios de descoberta de conhecimento deve ser efectuada por pessoa habilitada e de confiança, sujeita a controlos rigorosos, e sempre que possível, usando algoritmos de ocultação de identidade das pessoas envolvidas.

### **VI. 3 Riscos**

As ferramentas que temos vindo a apresentar são formas poderosas de descoberta de conhecimento que tenta ser escondido pelos seus autores. Como ferramenta poderosa na área dos serviços de Informações, acarreta sempre uma suspeita de uso abusivo, tema este sempre presente no debate sobre o seu emprego.<sup>75</sup> De facto apresentamos, de seguida, os riscos que se correm com a utilização destas técnicas. Na

---

<sup>75</sup> A UE mandatou uma comissão do Parlamento europeu para “confirmar a existência do sistema de interceptação de comunicações conhecido por ECHELON, cujo funcionamento é descrito no relatório STOA sobre o desenvolvimento da tecnologia de vigilância e riscos de abuso de informações económicas; verificar a compatibilidade de tal sistema com o direito comunitário, designadamente com o artigo 286º do Tratado CE, com as Directivas 95/46/CE e 97/66/CE, e ainda com o nº 2 do artigo 6º do Tratado UE à luz das seguintes questões:

- Os direitos dos cidadãos europeus encontram-se protegidos das actividades dos serviços secretos?
- A criptagem constitui uma protecção adequada e suficiente para garantir a defesa da vida privada dos cidadãos, ou deverão ser adoptadas medidas complementares e, em caso afirmativo, que tipo de medidas?
- De que modo poderão as Instituições da UE ser alertadas para os riscos decorrentes de tais actividades, e que medidas poderão ser adoptadas?
- Verificar se a interceptação de informações a nível mundial constitui um risco para a indústria europeia;
- Formular, eventualmente, propostas de iniciativas políticas e legislativas.

O relatório está disponível em [www.europarl.eu.int/tempcom/echelon/pdf/rapport\\_echelon\\_pt.pdf](http://www.europarl.eu.int/tempcom/echelon/pdf/rapport_echelon_pt.pdf), com o n.º PE 305.391.

secção seguinte apresentaremos também o que pode ser desenvolvido, ao nível da tecnologia, para obviar estes riscos.

### **VI. 3. 1 O fim da “privacidade”?**

A privacidade das pessoas é um bem que, nas sociedades ocidentais, é muito valorizado, sendo considerado um dos valores que define a liberdade da pessoa e das sociedades ao ponto de considerarmos como evoluídas, as sociedades que respeitam a privacidade dos seus cidadãos. Porém, a privacidade é um conceito subjectivo, depende da percepção de cada cidadão, da sua cultura, das convicções religiosas, entre muitos outros factores. Não se insere no âmbito deste trabalho dissertar sobre o conceito de privacidade, problemática abordagem do conceito de «vida privada» subjacente ao artº 35, nº 3 da CRP. Como refere Garcia Marques «na falta de definição do conceito de vida privada, noção erichada de dificuldades e, por isso mesmo, não operativa, torna-se bastante penoso alcançar com precisão a delimitação de fronteiras entre a "vida privada" e outros conceitos que vêm enunciados na al. b), como é o caso do "estado de saúde" e da "situação patrimonial e financeira"». A doutrina tem considerado de difícil definição o conceito de «privacidade», nomeadamente quando se pretende construir um regime jurídico coerente e «coeso».<sup>76</sup>

A privacidade e a segurança são conceitos que, muitas vezes, estão em contradição e requerem um tratamento equilibrado, devendo ser consideradas duas obrigações complementares do Estado junto dos seus cidadãos.

O uso de novas tecnologias poderá registar dados de diversa ordem da pessoa. O próprio bilhete de identidade pode conter dados que, para alguns fundamentalistas da privacidade, podem ser considerados uma invasão à sua privacidade. Os sistemas de registo em hotéis, passagens de avião, o registo de posições de telemóvel, o registo das compras através de cartão de crédito, podem ser consideradas uma invasão na vida privada, mas nem por isso, podem deixar de ser implementadas. Todas estas formas de registo existem, são necessárias ao bom funcionamento destes sistemas e continuarão a existir, no actual estado de desenvolvimento tecnológico, tendendo mesmo a generalizar-se a outros aspectos da vida.

Como veremos nas secções seguintes, o Governo não necessita de recolher mais informação sobre as pessoas para, «ligando os pontos», a poder analisar e transformar

---

<sup>76</sup> Comissão nacional de Protecção de dados pessoais. Disponível em <http://www.cnpd.pt/actos/aut/1997/aut059-97.htm>, em que se pode acompanhar uma discussão legal sobre a privacidade.

em conhecimento.<sup>77</sup> Necessita sim de autorização legal e de mecanismos de controlo para poder relacionar um enorme volume de informação, que se encontra disperso e sujeito a legislação específica, de forma a obter Informação relevante em áreas muito sensíveis como o terrorismo, crime organizado, lavagem de dinheiro, tráfico de seres humanos, crimes ambientais.

Reconhecemos que o acesso a um volume de informação tão diverso, não está isento de riscos de uso abusivo e de pesquisas da vida privada de “pessoas públicas”, podendo, no limite, ser usado com fins ilegais de manutenção ou derrube de governos.

### **VI. 3. 2 Falsos positivos e falsos negativos**

Um falso positivo acontece quando o processo reporta, de forma incorrecta, que encontrou o padrão que se procurava. Nos falsos negativos o processo indica o contrário, que não encontrou qualquer padrão, também de forma incorrecta.

Como o *data mining* é um processo de procura de padrões, não existem mecanismos que impeçam o sistema de reportar um padrão de comportamento típico de terroristas, num cidadão sem qualquer ligação a grupos criminosos. Outro problema pode acontecer com todos aqueles que têm ligações com os grupos criminosos fruto da sua actividade quotidiana. Se alguém arrendar casas ou alugar carros a terroristas, pode ser objecto de pesquisa sem qualquer fundamento. Aqui coloca-se um dos maiores desafios ao sistema: reduzir ao máximo a ocorrência de falsos positivos.

Os falsos negativos, por outro lado, não causam tantas preocupações de legalidade. De facto se o sistema indica que não encontrou nenhum padrão, os serviços não vão colocar ninguém sob vigilância. Não deixa de ser um problema e um desafio ao sistema evitar que existam falsos negativos, pois pode comprometer o seu funcionamento e a segurança do país.

Como já foi referido, estas ferramentas devem ser consideradas como poderosos meios de ajuda aos analistas e investigadores dos serviços encarregados da Segurança e da Defesa Nacional, produzindo pistas que permitam uma investigação posterior e uma confirmação, ou não, por meios tradicionais.<sup>78</sup> Neste caso os falsos positivos podem ser descobertos antes de terem um impacto significativo na vida das pessoas. Todavia, se forem disseminados por outros serviços ou forças policiais, sem serem devidamente confirmados, pode ser muito difícil evitar causar danos às pessoas, contribuindo para o

---

<sup>77</sup> Cf. Op. Cit., TAIPALE, 2003, 50 e ss.

<sup>78</sup> Cf. Op. Cit., DeROSA, 2004, 15.

emprego de recursos de pesquisa de Informações em situações erróneas, causando mal-estar nos agentes do sistema.

### **VI. 3. 3 Uso inadequado da Informação**

A concentração da informação, seja em *data warehouses* físicas ou virtuais, é sempre susceptível de uso abusivo por parte de pessoas ou entidades que lhe tenham acesso. Pode existir a tentação de se criar um «*big brother*», na expressão Orwelliana, que pesquise informações ou padrões de comportamento que não põem em causa segurança nacional, antes favorecem a acção dos governos, grupos de pressão ou, ainda, a chantagem sobre certas pessoas.

Os serviços de Informações são uma das formas de poder do Estado e, como tal, devem ser usados com resguardo da salvaguarda da legalidade, necessidade e pelo respeito das liberdades e garantias dos cidadãos.

Como a história mostra, num extremo, os Serviços de Informação podem constituir-se como centros de poder dentro do Estado, independentes do sistema político, enquanto, noutro extremo, podem servir o aparelho governativo para se perpetuar no poder. Na história de Portugal não é difícil encontrar exemplos de uso desregrado de Informações, em benefício do poder instalado.<sup>79</sup> O General Pedro Cardoso explica que Portugal teve, nos últimos cinco séculos, três séculos de censura prévia e uso abusivo de Informações por parte de diversos governos.<sup>80</sup> Já em época de pleno regime democrático, Portugal viveu estigmas antigos com as notícias que ficaram conhecidas como “SIS – Universidade Moderna” e “SIEDM – Veiga Simão”.<sup>81</sup>

Devemos realçar que os sistemas de descoberta de conhecimento não pretendem recolher mais informação, antes dispor da informação existente actualizada e em tempo, tendo objectivos determinados à priori e serem supervisionados pelo poder judicial. Assim, o uso indevido de Informação pode acontecer, não porque se recolhe mais informação sobre factos que afectem a vida privada das pessoas, mas porque os agentes intervenientes no processo usam a informação cruzada possibilitando o conhecimento de informações não relevantes para os objectivos iniciais, mas tentadora nos planos

---

<sup>79</sup> Mesmo nos EUA, onde há uma grande tradição democrática, houve tentativas de uso dos Serviços de Informação para apoio das actividades de obtenção de Informações de “adversários” políticos sendo o caso Watergate, que levou à resignação do presidente Nixon, o mais emblemático.

<sup>80</sup> Entrevista a Pedro Simões em 2001. Cf. Op. Cit., SIMÕES, 2002, 39 e ss.

<sup>81</sup> Cf. Op. Cit., SIMÕES, 2002, 128 e 129.

políticos, financeiros ou até criminais. Há sempre a tentação de expansão do sistema a áreas diferentes das inicialmente previstas.<sup>82</sup>

O controlo e supervisão do uso destas ferramentas deve ser efectuado a vários níveis, interno e externo. Como veremos há algumas respostas, baseadas nas tecnologias mais recentes que podem ser implementadas, para atenuar os riscos apresentados.

#### **VI. 4 Atenuar os riscos**

As formas de minimizar os riscos enumerados na secção anterior devem ser baseadas na tecnologia, na definição de um quadro legal coerente, na selecção correcta dos intervenientes no processo e na protecção física das instalações e dos dados.

Neste trabalho limitarmo-nos-emos a tecer considerações baseadas na tecnologia abordando as áreas em desenvolvimento que permitem o tratamento de informação de forma anónima, a redução de falsos positivos e tecnologias que permitam auditar e criar regras de uso e processamento de bases de dados. Todos estes subsistemas encontram-se já implementados, com diferentes graus de desenvolvimento, nas modernas bases de dados comerciais.

A primeira área de desenvolvimento tecnológico é a do tratamento anónimo de dados, para mascarar a informação de identificação do registo, de forma aos analistas poderem efectuar as suas pesquisas sem acederem à identidade real das pessoas. Um exemplo é o que ocorre com um aluno que executa um exame e a sua correcção é efectuada apenas conhecendo um número de teste. Claro que quando falamos em informações provenientes de múltiplas bases de dados o problema torna-se mais difícil de resolver. O primeiro passo a implementar consiste no mascaramento de elementos da identidade - tais como, nomes, endereços, números de bilhete de identidade, carta de condução, entre outros - através de códigos. Isto não resolve o problema por completo. Pode-se inferir a identidade de uma pessoa através do sexo, data de nascimento, local de trabalho, função que desempenha, etc. Para obviar este problema tem-se desenvolvido algoritmos de protecção de privacidade dos quais se destaca o “K-anonymity”, desenvolvido por Latanya Sweeney na Carnegie Mellon University, EUA<sup>83</sup>. Este algoritmo permite evitar que se tenha acesso a dados que identifiquem uma pessoa dentro de um grupo de K-1 outros indivíduos. Por exemplo se K for definido como

---

<sup>82</sup> Cf. nota 75 da página 49.

<sup>83</sup> O trabalho de Latanya Sweeney tem sido empregue pelo DARPA no seu programa de TIA. Encontra-se em Anexo C a explicação do algoritmo. Há outras formas de protecção de dados desenvolvidos para a manipulação de dados usando o KDD. A discussão destes métodos pode ser acompanhada em [www.markle.org](http://www.markle.org).

10000, só podemos inferir identidades num grupo de 10000 pessoas.<sup>84</sup> O K é assim definido de acordo com os decisores políticos e com o decorrer da investigação. Quando se começa a procurar um padrão, K deve ter um valor muito elevado, à medida que se vão eliminando registos o K deve ir diminuindo de forma a chegar a um ponto em que existe um número de suspeitos passível de poder ser investigado por métodos tradicionais. Este método é conhecido como revelação selectiva,<sup>85</sup> em que os investigadores vão tendo conhecimento das identidades à medida que a investigação vai progredindo. A autorização concedida aos investigadores deve partir das entidades competentes, e as identidades só devem ser reveladas quando existirem certezas razoáveis sobre as actividades ilegais que se procuram.

A resolução de falsos positivos está directamente relacionada com o primeiro passo do KDD, em que a qualidade dos dados e a quantidade de “ruído” existente pode provocar distorções na pesquisa de padrões. Um dos programas mais complexos que está a ser desenvolvido em diferentes universidades e no DARPA é a criação de sistemas inteligentes que possam correlacionar dados de diferentes bases de dados sem duplicação de registos fruto da falta de normalização existente. Uma solução para o problema da normalização seria a criação de uma norma que implementasse um conjunto de procedimentos de recolha de informação. Este processo é de implementação relativamente demorada, tem problemas de natureza legal e os resultados seriam sempre medíocres pois muitos dos erros de colecta de informação provêm dos operadores de registo de dados.<sup>86</sup>

A terceira área de desenvolvimento prende-se com os sistemas de auditoria. O controlo de acessos aos dados, em grandes bases de dados, é um processo comum na maioria das empresas comerciais, e é obrigatória a sua implementação nas bases de dados dos mercados financeiros. O sistema de auditoria permite conhecer quem acede aos dados, quais as pesquisas efectuadas, as horas a que o sistema recebeu ou forneceu informação e de onde foi acedido. Por esta razão, auditar dados pode ser também uma fonte de informação, pois pode-se conhecer as investigações em curso, quem as está executar, requerendo que os auditores sejam pessoas de idoneidade a toda a prova. É um mecanismo poderoso e eficaz de controlo da informação, requerendo o consumo de grandes recursos computacionais e humanos.

---

<sup>84</sup> Cf. Op. Cit., DeROSA, 2004, 18.

<sup>85</sup> Cf. Op. Cit., TAIPALE, 2003, 74 e 79.

<sup>86</sup> Vide nota 68, p. 46.

O último desenvolvimento tecnológico que vamos abordar prende-se com a implementação de regras de acesso e pesquisa, que permitam a protecção da privacidade. Este sistema apoia-se em dois elementos. Primeiro, as pesquisas são efectuadas de acordo com as permissões do utilizador ou da entidade que efectua a pesquisa, através de agentes inteligentes que são agregados à pergunta. Ou seja, uma pesquisa efectuada de acordo com uma autorização atribuída a um utilizador pode ter permissões diferentes da mesma pergunta que tenha autorização atribuída por uma entidade jurídica. Em segundo lugar, os dados podem ser etiquetados com meta-dados (dados sobre os dados), descrevendo como podem ser processados. Assim, mesmo que os dados sejam copiados para uma base de dados diferente, mantêm as regras pelas quais podem ser processados garantindo a sua protecção inicial. O processamento de dados baseados em regras assenta em ferramentas de etiquetagem e filtragem de dados.<sup>87</sup>

## **VI. 5 O estado da arte**

Ao longo deste capítulo temos vindo a analisar um sistema de pesquisa de conhecimento baseado na mais moderna tecnologia de bases de dados e nos avanços matemáticos na área da teoria dos conjuntos. Estes sistemas têm sido desenvolvidos comercialmente pela indústria da publicidade e nas pesquisas de mercado. O grande objectivo é conhecer padrões de consumo e padrões de comportamento face às promoções de vendas. Já mostrámos que todas as cadeias de supermercados disponibilizam um cartão de cliente para poder obter dados de consumo do cliente.

O desenvolvimento das ferramentas de KDD, permitiu o seu emprego em áreas tão diversas como a medicina, na banca, nas telecomunicações, nas bibliotecas, etc. Actualmente estes processos estão a ser usados para as empresas obterem conhecimento do mercado e dos seus concorrentes directos e é também empregue nas áreas de Segurança e Defesa, como temos visto. Os EUA lideram as pesquisas efectuadas neste domínio, mas o Reino Unido, a Austrália, o Canadá, a França, a Espanha entre outros países desenvolvidos, têm programas com grande apoio das TIC, nomeadamente sistemas de descoberta de conhecimentos em bases de dados.

---

<sup>87</sup> O sistema de filtragem de dados DCS-100 (“Carnivore”) é um sistema de filtragem analítica de dados desenhado para examinar tráfego de correio electrónico e só recolher o material que está autorizado. “O Carnívoro fornece ao FBI a possibilidade de interceptar e recolher comunicações que se encontrem sob a alçada da lei, enquanto ignora as comunicações que não são autorizadas interceptar. Funciona como os “sniffers” comerciais e outra ferramentas de diagnóstico de rede usadas pelos fornecedores de serviço de Internet”. Cf. Op. Cit., TAIPALE, 2003, 78. Tradução do autor.

Ao nível tecnológico os principais fabricantes de bases de dados, Oracle, IBM, Sybase, implementaram mecanismos de *data mining* embebidos nos seus motores de pesquisa comerciais e têm sistemas que permitem auditar o seu acesso. O desenvolvimento matemático na área da teoria de conjuntos, da estatística e da algoritmia, permite-nos crer que é possível efectuar buscas de padrões complexos sem invadir a privacidade das pessoas e sem a criação de falsos positivos que tornem impossível a implementação do sistema.

A formação dos utilizadores de um sistema de KDD é complexa. Deve promover um conhecimento profundo de pesquisas em bases de dados relacionais e orientadas a objectos, o conhecimento da legislação que lhe permita aceder a dados e ter formação na área de análise de Informações. Cremos que o ideal será formar equipas pluridisciplinares com uma forte componente tecnológica. No Centro de Informática do Exército existe uma máquina com capacidade computacional para efectuar estes cálculos e com as mais modernas versões da base de dados da IBM.

## **VI. 6 Síntese conclusiva**

A informação armazenada nas bases de dados dos diferentes serviços de um país pode conter conhecimentos valiosos na área da prevenção e Segurança. O cruzamento desta informação com aquela que está disponível em fontes abertas e a que está armazenada em entidades privadas pode ser crucial para detectar factos e pessoas que ameacem a Segurança Nacional.

O governo não necessita de recolher mais informação para poder aplicar novas técnicas de descoberta de conhecimento, antes, impõe-se a criação de mecanismos legais que o permitam, é necessário recrutar pessoal muito especializado, implementar algoritmos de protecção de privacidade e aceitar correr alguns riscos com falsos positivos, pelo menos na fase de implementação do sistema, quando os analistas ainda não estão habituados a destrinçar o “ruído” do sistema.

Para aumentar a eficiência destes sistemas dever-se-à obter padrões, o mais exactos possíveis, pelo que a análise exaustiva de casos passados e a cooperação internacional são imprescindíveis. A busca de padrões de forma não supervisionada numa base de dados requer uma experiência muito grande e uma capacidade de computação muito elevada. Há bibliografia disponível com padrões referentes a lavagem de dinheiro, tráfico de seres humanos e de armas. Quanto à ameaça terrorista ainda não foi publicado nenhum artigo de fundo de análise de padrões. Duas razões

levam-nos a acreditar que ainda levará tempo a esses padrões estarem disponíveis. A primeira prende-se com o carácter sigiloso do comportamento dos terroristas. Na área das Informações, como sabemos, o segredo é a alma do negócio. A segunda razão decorre da necessidade de criar rotinas de pesquisa que permitam o estabelecimento de padrões, função sempre demorada.

A adopção de análise de informação por *data mining* não retira responsabilidade ao analista, mas facilita o seu trabalho e, porventura, pode ser a diferença entre a Informação chegar em tempo oportuno ou não.

Os cidadãos deverão compreender que estes sistemas não são uma nova invasão da sua privacidade. Se usados correctamente são bons meios de avaliação de ameaças, se usadas com má-fé, claro, que podem causar danos aos cidadãos. Mas todos os sistemas podem, se usados para fins maléficos, causar escolhos e problemas graves.

“Os descobrimentos do século XV foram uma façanha de gente metódica, dotada de clara inteligência política, de visão lúcida, muito precisa, dos escopos práticos a que tendia e do estudo minucioso dos meios adequados a tais escopos; em suma, um vasto plano conjunto, capacidades raras de organização”

António Sérgio<sup>88</sup>

## VII. CONCLUSÕES

Em todos os tempos se procurou conhecer as ameaças à segurança dos povos e os modos de evitar que se concretizassem. Até há bem pouco tempo as ameaças eram identificadas como entidades precisas – Estados, organizações mais ou menos institucionalizadas e reconhecidas – e por isso era para elas que se dirigiam as investigações e desenvolvimentos técnicos na recolha de informação.

Com o fim da guerra fria e o advento do século XXI as ameaças mudaram, são agora mais difusas na sua identidade e, como tal, mais difíceis de identificar e, por isso, de estudar.

Apesar de continuar a ser um meio eficaz e necessário, o emprego de agentes infiltrados nas organizações terroristas e de crime organizado transnacional é muito difícil de concretizar. É um processo muito demorado, com resultados a longo prazo pelo que, os Estados têm de lançar mão de outros meios de obter informações credíveis, relevantes e oportunas que lhe permitam garantir a segurança dos seus cidadãos face ao terrorismo, ao narcotráfico, à proliferação de ADM, à fraude económica e fiscal, aos ataques aos sistemas informáticos e outras ameaças que, mercê da globalização, chegam hoje a todos os recantos do planeta.

Um dos meios mais poderoso de armazenagem de informação está hoje disponível nas imensas bases de dados e a sua análise, pelos processos de *data mining*, poderá tornar essa informação altamente eficaz na identificação de ameaças latentes ou declaradas. Através do estudo de padrões e assuntos, por pessoal especializado, podem inferir-se situações de ameaça à Segurança e apresentar às instância de decisão dados precisos sob quem deve ser considerado suspeito e ser colocado sob vigilância, ou que actividades devem ser colocadas sob investigação por parte dos meios convencionais de vigilância.

---

<sup>88</sup> SÉRGIO, António, *Breve Interpretação da História de Portugal*, 8.ª Edição, Lisboa, ed. Sá da Costa, 1978, p. 44.

É claro que estamos perante processos complexos e que não estão isentos de erro, mas que, face à escassa e difícil recolha de informação sobre as ameaças actuais, é um bom instrumento de trabalho que está ser posto ao serviço por inúmeros Estados.

A investigação efectuada e o estudo realizado, tendo como amarras as hipóteses orientadoras do trabalho, impõe a sistematização dos aspectos mais relevantes:

- A legislação que enquadra o SIRP ainda não reflecte as transformações ocorridas no ambiente estratégico internacional. Necessita de uma revisão à luz das novas ameaças, à luz das revoluções tecnológicas, entretanto, ocorridas e à das novas responsabilidades assumidas por Portugal, com a presença de forças militares nos «quatro cantos do mundo»;
- Os sistemas de descoberta de conhecimento e bases de dados podem ser uma ajuda incalculável no processo de análise de ameaças. Os meios informáticos, quer de *hardware*, quer *software*, estão disponíveis concomitantemente com um manancial de informação tanto em entidades públicas como privadas;
- A análise de informação através de poderosos sistemas de *data mining* agita sempre a dialéctica segurança versus privacidade. Mostrámos que, apoiados em forte tecnologia e na melhor algoritmia, é possível efectuar buscas de padrões sem ferir as liberdades e os direitos dos cidadãos. Cremos que é possível implementar sistemas de KDD sem invasão da privacidade daqueles que se pretende manter em segurança;
- A separação de Informações em estratégicas, operacionais ou táticas é, cada vez mais, artificial. Informações são Informações e, no contexto actual, todas são importantes. Por isso, é imperativo a partilha de Informações pelos serviços encarregues de a produzir. Não devem existir receios de uso abusivo de informação, antes se devem desenvolver normas de controlo mais eficazes;
- A reestruturação do SIRP não pode ficar alheia ao domínio das novas tecnologias. Quem dominar a informação pode produzir Informações em tempo útil e extrair conhecimento donde muitos pensam que só há «ruído». É um desafio que Portugal não pode perder, e à imagem dos descobrimentos do século XV, necessitam de uma visão lúcida, persistência, organização e de um plano conjunto.

## Propostas e Recomendações

O trabalho realizado, de cariz essencialmente académico, não é de natureza a incluir propostas, porém é nossa intenção ousar um pouco mais, aventurar o nosso contributo para um melhor sistema de análise das ameaças à Segurança e à defesa Nacional.

- Mantendo o respeito pela privacidade dos cidadãos e em nome da sua segurança o Estado Português deve juntar-se aos seus parceiros internacionais criando um sistema de estudo de Informações em *data mining* e formando os seus agentes para este novo e prometedor meio de controlo de ameaças à Segurança Nacional. Deverá, também, prever como vai proteger os dados recolhidos e evitar o seu uso abusivo, o que requererá, não só uma responsabilização dos agentes, mas também a criação de mecanismos informáticos de protecção.
- Portugal deve colaborar no desenvolvimento dos sistemas de Indicadores e avisos da NATO. A colaboração deverá ser ao nível de pessoal de Informações e ao nível de pessoal informático. O NIWS da NATO é uma ferramenta poderosa e é muito importante que Portugal participe com Informações próprias a todos os níveis.
- A formação académica nas áreas da inteligência artificial e da matemática computacional são a base de um bom emprego dos sistemas de *data mining*. O Exército tem oficiais bem preparados para poderem abordar estas áreas. Pode assim, dar um contributo decisivo na efectivação de um sistema de pesquisa de conhecimento.
- Do CEM<sup>89</sup> retiramos que as FA devem abandonar um modelo assente em estruturas estáticas, devendo, sobretudo, preocupar-se com as novas ameaças e com o desempenho de missões no EEINP e EEINC. Para isso, têm que ter Informações a todos os níveis. É muito temerário atribuir uma missão a uma força militar sem primeiro esclarecer a situação e avaliar as ameaças que essa força pode ter que enfrentar. Aliás, não pode haver um planeamento de forças sem se conhecer a ameaça. Por estas razões as FA em geral e o Exército em particular devem participar desde todo o tempo e em todas as estruturas de pesquisa e análise de Informações.

---

<sup>89</sup> Cf. CEM, p.6

- A criação de uma autêntica comunidade de Informações é um imperativo. Tal como em muitas outras actividades, as Informações exigem pessoal especializado e que se conheça mutuamente para poderem confiar uns nos outros. Um bom analista nunca está formado. Tem sempre mais a aprender, novos meios a estudar. O Exército deve olhar para esta comunidade e ajudar a implementá-la.
- Deve ser implementado um sistema nacional de análise de Informação conjunto, à imagem do que têm feito os nossos parceiros europeus. Este sistema deverá ter um enquadramento legal adequado e ser operado por pessoas com formação específica.

Analisar e avaliar as ameaças sempre foi uma tarefa ingrata. O analista diz o que espera que vá acontecer, o que prevê, sem ainda ter acontecido. Se a prevenção for eficaz e a ameaça não se tornar em agressão fica sempre a dúvida se o analista estava certo ou não. Neste trabalho apresentámos o que consideramos ser o estado da arte na avaliação e descoberta de novas ameaças. Estamos conscientes que muito ficou por dizer. A vasta bibliografia encontrada, o grande desenvolvimento tecnológico, o carácter pluridisciplinar desta temática impossibilitou-nos de efectuar uma investigação mais profunda. Estamos cientes que num futuro recente a tecnologia pode tornar o nosso trabalho obsoleto e até suscitar sorrisos a quem o ler.

## BIBLIOGRAFIA

AAVV, Nato Intelligence Warning System, MC 166, NATO, 2004.

AAVV, NATO Glossary of Terms and Definitions, AAP-6, NATO, 2004.

BERKOWITZ, Bruce D., GOODMAN, Allan E., *Strategic Intelligence for American National Security*, 1.<sup>a</sup> ed. New Jersey, Ed Princeton University Press, 1989. ISBN 0-691-07805-X.

BORGES, Mafalda de Sampaio, *Nótulas para um novo Conceito Estratégico de defesa Nacional – As Informações para o Século XXI*, in Revista Militar n.º 12, Lisboa, Dezembro 2003, pp. 1257-1264.

CHAVES, Carlos, *Tendências organizacionais dos Sistemas de Informações militares. Que modelo para o futuro. Articulação com as organizações Internacionais*. TILD, CSCD 2003/2004, IAEM, Lisboa, 2004.

COUTO, Abel Cabral, *Elementos de Estratégia – apontamentos para um curso*, Vol. 1, IAEM, Lisboa, 1998.

FAYYAD, Usama M. et al., *Advances in Knowledge Discovery and Data Mining*, ed. MIT, Massachusetts, 1996, ISBN 0-262-5609-6.

GROTH, Robert, *Data Mining: A Hands-On Approach for Business professionals*, Ed. Prentice-Hall, New Jersey, 1997, ISBN 0-13-756412-0.

GUEHENNO, Jean-Marie, *Sécurité et globalisation* in *Les Guerres qui menacent le Monde*, Ed. Du Félin, Paris, 2001. ISBN 2-86645-400-6.

HERMAN, Michael, *Intelligence Power in Peace and War*, 1<sup>a</sup> Edição, Cambridge, Ed. Cambridge University Press, 2003. ISBN 0-521-56636-3.

KRAFT, TCor Uwe, *A Análise da Política de Segurança e defesa da Alemanha*, CEM, 2003/004, documento policopiado.

MOREIRA, Adriano et al., *A Defesa Nacional e as Forças Armadas in Estratégia*, Vol. XIV, ed. IPCE, Lisboa, 2003. ISSN 1645-9083.

PINTO, Valença, *Segurança e Defesa*: in Vários, *Estratégia*, nº 16 – 1º Semestre, Instituto de Estudos Estratégicos e Internacionais, 2002.

RAFFARIN, Jean-Pierre, *La politique de défense de la France*, in *Défense Nationale*, Paris, Novembro 2002. ISSN 0336-1489.

RAMALHO, TGen Pinto, “*A crise Internacional – a sua Gestão*”, in *Estratégia*, Vol. XII, Ed. IPCE, Lisboa, 2000.

RAMONET, Ignacio, *Des nouveaux intérêts stratégiques* in *Les Guerres qui manacent le monde*, Éditions du Félin, Paris, 2001, ISBN: 2-86645-400-6.

RODRIGUES, Alexandre Reis, *Nos meandros da política de defesa*, Editorial Notícias, Lisboa, 2002. ISBN 972-46-1400-X.

ROGEIRO, Nuno, *Guerra em Paz – A Defesa Nacional na Nova Desordem Mundial*, 1ª edição, Lisboa, Hugin Editores, 2002. ISBN 972-794-140-0.

SANTOS, José Alberto Loureiro dos, *Reflexões sobre Estratégia – Temas de Segurança e defesa*, Mem Martins, Ed. IAEM e Publicações Europa-América, 2000. ISBN 972-1-04718-X.

\_\_\_\_\_, *A Idade Imperial: a nova era, Reflexões sobre Estratégia III*, Mem Martins, Ed. Publicações Europa-América, 2003. ISBN 972-1-05178-0.

\_\_\_\_\_, *Convulsões: Ano III da «Guerra» ao terrorismo – Reflexões sobre Estratégia IV*, Mem Martins, 5ª ed., Ed. Publicações Europa-América, 2004. ISBN 972-1-05382-1.

SÉRGIO, António, *Breve Interpretação da História de Portugal*, 8.<sup>a</sup> Edição, Lisboa, Sá da Costa, 1978. ISBN 972-562-021-6.

SHULSKY, Abram N. e SCHMITT, Gary J., *Silent Warfare – Understanding the World of Intelligence*, 3.<sup>a</sup> Edição, Washington D.C., Ed. Brassey's, 2002. ISBN 1-57488-345-3.

SIMÕES, Pedro, *Os Serviços Secretos em Portugal*, 1.<sup>a</sup> ed., Lisboa, Ed. Prefácio, 2002. ISBN 972-8563-82-5.

VIANA, Cor. Vítor Daniel Rodrigues, *O Conceito de Segurança Alargada e o seu Impacto nas Missões e Organização das Forças Armadas*, Instituto de Altos Estudos Militares, Curso Superior de Comando e Direcção 2002/2003, Lisboa, 2003.

VIEIRA, José António da Silva, *O Sistema de Apoio à Decisão de Gestão no Exército Português. Contributos para um modelo mais operacional e eficaz*, TILD, CEM 2001/03, IAEM, Lisboa, 2002.

### **Artigos de periódicos**

FREIRE, Manuel Carlos, *Forças Armadas criam um novo serviço de Informações*, in Diário de Notícias, 20 de Setembro de 2004.

DUFFY, Michael, *How to Fix Our Intelligence*, Revista Time, Washington, D.C., vol. 163, n.º 17, 26 de Abril de 2004, pp.23-29.

### **Legislação**

- Lei constitucional n.º 1/2004, 24 de Julho – Constituição da República Portuguesa (CRP) (6.<sup>a</sup> Revisão).
- Lei n.º 29/82, 11 de Dezembro, (com seis alterações posteriores) – Lei da Defesa Nacional e das Forças Armadas (LDNFA).
- Lei n.º 20/87, de 12 de Junho, alterada pela Lei n.º 8/91, de 1 de Abril – Lei de Segurança Interna.
- Lei n.º 30/84, de 5 de Setembro, alterada pelas Leis n.ºs. 4/95, de 21 de Fevereiro, 15/96, de 30 de Abril, e 75-A/97, de 22 de Julho – Lei-quadro do Sistema de Informações da República Portuguesa (SIRP).

- Lei n.º 15/96, de 30 de Abril – Reforça as competências do Conselho de Fiscalização dos Serviços de Informações.
- Decreto-Lei n.º 254/95, 30 de Setembro – Lei Orgânica do Serviço de Informações Estratégicas de Defesa e Militares (SIEDM).
- Decreto-Lei n.º 225/85, de 4 de Julho, alterado pelos Decretos-Leis n.º 369/91, de 7 de Outubro, e 245/95, de 14 de Setembro – Lei Orgânica do Serviço de Informações de Segurança (SIS).
- Resolução do Conselho de ministros n.º 6/2003 – CEDN.
- Resolução do Conselho de Ministros n.º 22/98 – Regulamento do Centro de Dados do SIEDM.
- Conceito Estratégico Militar – aprovado pelo MEDN, 22 de Dezembro 2003.

### **Sítios da Internet**

BAIRD, Zoë, et al., *Protecting America's Freedom in the Information Age*, Markle Foundation Task Force, Nova York, Outubro de 2002, ISBN 0-9725440-0-3, disponível em: [http://www.markletaskforce.org/report1\\_overview.html](http://www.markletaskforce.org/report1_overview.html), consultado em 29 de Setembro de 2004.

Comissão Nacional de Protecção de dados pessoais. Disponível em <http://www.cnpd.pt/actos/aut/1997/aut059-97.htm>. Consultado em 29 de Setembro de 2004.

*CORAL - Money Laundry Pattern Learning and Detection Using Data Mining Techniques*, A aplicação tem uma versão de demonstração disponível em <http://www.fortune.binghamton.edu/demo/CoralDemo.html>, consultado em 29 de Setembro de 2004.

DeROSA, Mary, *Data Mining and Data Analysis for Counterterrorism*, Ed. Center for strategic and International Studies, Washington, D. C., 2004. ISBN 0-89206-443-9. Disponível em [www.csis.org](http://www.csis.org), consultado em 12 de Julho 2004.

GASPAR, Carlos, *O regresso do realismo*, IPRI, disponível em <http://www.ipri.pt/investigadores/artigo.php?idi=3&ida=48>. Consultado em 6 de Setembro de 2004.

GONÇALVES, Rodrigo e Hillesheim, *Sistemas de Informação inteligentes*, UFSC, Santa Catarina, 2003, disponível em [www.inf.ufsc.br/~rodrigog/free/TranspIA.pdf](http://www.inf.ufsc.br/~rodrigog/free/TranspIA.pdf). Consultado em 6 de Setembro 2004.

HUTCHINGS, Robert L., *Looking over the Horizon: Assessing America's Strategic Challenges*, Washington, D.C., 9 de Março de 2004, disponível em: [www.cia.gov/nic](http://www.cia.gov/nic), consultado em 14 de Junho de 2004.

i2 –Software de análise de ligações, disponível em [www.i2.co.uk](http://www.i2.co.uk), consultado em 29 de Setembro de 2004.

KRIENDLER, John, *Anticipating crises*, NATO Review, Inverno de 2002, disponível em <http://www.nato.int/docu/review/2002/issue4/english/art4.html>, consultado em 6 de Setembro de 2004.

LEWIS, James A., *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Ed. Center for strategic and International Studies, Washington, D. C., 2002. Disponível em [www.csis.org](http://www.csis.org), consultado em 12 de Julho 2004.

POINDEXTER, John, *Overview of the Information awareness Office*, Conferência DARPA Tech, Agosto de 2002. Disponível em [www.darpa.mil](http://www.darpa.mil). Consultado em 6 de Setembro 2004.

TAIPALE, K. A., *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, in Science and Technology Law Review, Columbia, Vol. V, 2003. Disponível em [www.stlr.org](http://www.stlr.org). Consultado em 6 de Setembro 2004.

TSA – Sítio oficial da Agência de Segurança de Transportes, [www.tsa.gov](http://www.tsa.gov). Consultado em 29 de Setembro de 2004.

Sítios da Internet que apresentam objecções fundamentadas ao programa TIA:

<http://www.nytimes.com/2002/11/14/opinion/14SAFI.html>;

<http://www.epic.org/privacy/profiling/tia/>;

<http://www.unknownnews.net/031001a-nt.html>, Consultados em 6 de Setembro 2004.

ZUJAR – Informações sobre o programa de *data mining* da administração tributária de Espanha em <http://www.dgci.min-financas.pt/ciat/DocsTecnico/espanhol/1espana.doc>, consultado em 29 de Setembro de 2004.

### **Entrevistas realizadas:**

Cor. Sousa Teles, Comandante do Regimento de Artilharia N.º 5, em 23 de Dezembro de 2003.

Dr. Yoram Kahati, *Institute for Counter-Terrorism*, Israel, em 19 de Maio de 2004.

Maj. Alves, 2º comandante do BISM, em 4 de Junho de 2004.

TCor. Dias Bento, DIMIL, em 31 de Julho de 2004.

TGen Vizela Cardoso, Director do IAEM, em 23 de Setembro de 2004.

### **Bibliografia auxiliar**

APOLINÁRIO, Cor. Manuel António, *A globalização nos Cenários Estratégicos e a sua Influência no Sistema de Defesa Nacional*, TILD, CSCD 2001/2002, IAEM, Lisboa, 2002.

BINDER, Patrice e LEPICK, Olivier, *Les armes biologiques*, Publications Universitaires Françaises, Paris, 2001, ISBN :2-13-052588-6.

CEPIK, Marco, *Inteligência e Políticas Públicas: dinâmicas operacionais e condições de legitimação*, In *Security and Defense Studies Review*, Vol. 2 Inverno 2002/2003, pp 256-267.

CHAUPRADE, Aymeric, *Géopolitique: constantes et changements dans l'histoire*, Ed. Ellipses, Paris, 2001, ISBN: 2-7298-0668-7.

CHED. *Etudes Sur l'Histoire due Reinseignement*, La Vauzelle, Paris. 1998, ISBN: 2-7025-0432-9.

LOPES, Maj. José Augusto Amaral, *Contributos para a Implementação de um Sistema Nacional de Gestão de Crises*. TILD, CEM 2001/2003, IAEM, Lisboa, 2003.

MONTEIRO, Cor. Artur Neves Pina, *A Estratégia Militar Face à Revisão dos Sistema de Gestão de Crises da OTAN e da Defesa Militar Contra o Terrorismo*. TILD, CSCD 2002/2003, IAEM, Lisboa, 2003.

MAYER, Claude 2001, *L'Arme Chimique*, Edition Ellipses, Paris, 2001, ISBN 2-7298-0837-X.

SILVA, Maj. Paulo Jorge Lopes da, *A participação das Forças Armadas em missões de Segurança Interna: implicações para o Exército*, TILD, CEM 2002/2004, IAEM, Lisboa, 2004.

WARUSFEL, Bertand, *Contre Espionage et Protection du Secret - Histoire, droit et organisation de la sécurité nationale en France*, La Vauzelle, Paris, 2000, ISBN 2-7025-0451-5.

## ÍNDICE DE APÊNDICES

Apêndice 1 – Orgânica do SIRP (Comentários) .....	Apd 1 / 1
Apêndice 2 – Matriz de comparação de <u>novas</u> ameaças .....	Apd 2 / 1
Apêndice 3 – Avaliação por assuntos ou ligações dos atentados de 11 de Setembro...	Apd 3 / 1

## ÍNDICE DE ANEXOS

Anexo A – Cópia do artigo do <i>The Observer</i> – Clima como maior ameaça.....	Anx A / 1
Anexo B – Modelo proposto pelo Cor Carlos Chaves para o SIRP .....	Anx B / 1
Adenda A – Modelo do Sistema de Informações da República .....	Anx B / 3
Adenda B – Proposta de Constituição do Conselho Superior do Sistema de Informações da República (CSSIR).....	Anx B / 4
Adenda C – Proposta do Conselho Executivo do Sistema de Informações da República (CESIR) .....	Anx B / 5
Anexo C – k-ANONYMITY; um modelo de protecção da privacidade .....	Anx C / 1

Apêndice 1 – Orgânica do SIRP (Comentários)

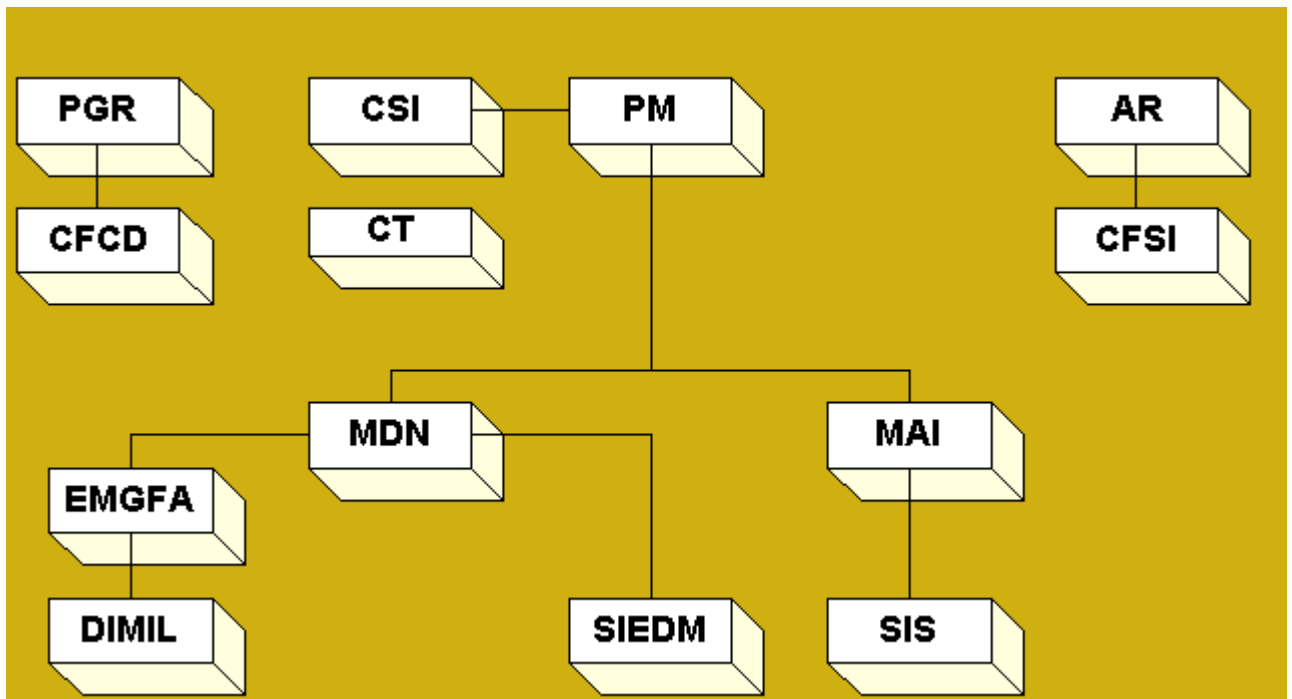


Fig 1 – Orgânica do SIRP (fonte: [www.sis.pt/sirp/orgsirp.htm](http://www.sis.pt/sirp/orgsirp.htm), consultado em 09/Set/2004)

<b>AR</b>	- Assembleia da República.	<b>MDN</b>	- Ministro da Defesa Nacional
<b>CFSI</b>	- Conselho de Fiscalização dos Serviços de Informações	<b>EMGFA</b>	- Estado-Maior-General das Forças Armadas
<b>PGR</b>	- Procuradoria-Geral da República	<b>DIMIL</b>	- Divisão de Informações Militares
<b>CFCD</b>	- Comissão de Fiscalização dos Centros de Dados	<b>SIEDM</b>	- Serviço de Informações Estratégicas de Defesa e Militares
<b>PM</b>	- Primeiro-Ministro	<b>MAI</b>	- Ministério da Administração Interna
<b>CSI</b>	- Conselho Superior de Informações	<b>SIS</b>	- Serviço de Informações de Segurança
<b>CT</b>	- Comissão Técnica		

Comentários:

1. A DIMIL apesar de se encontrar graficada não faz Parte do SIRP, conforme está estipulado no artigo 13.º, em conjugação com o art.º 2 da lei quadro do SIRP.
2. A DIMIL tem as suas funções estipuladas no artigo 14.º, Decreto-Lei n.º 48/93 de 26 de Fevereiro, Lei Orgânica do Estado-Maior-General das Forças Armadas.
3. O CFSI não tem competências de verificação sobre as Informações obtidas pela DIMIL.
4. A DIMIL colabora com SIRP, institucionalmente e oficiosamente, e é chamada a pronunciar-se sobre diplomas do SIRP.

## Apêndice 2 – Matriz de comparação de novas ameaças

No presente apêndice efectuamos uma comparação das novas ameaças consideradas mais relevantes para o emprego das FA. Os EUA não foram incluídos pois a ameaça que mais preocupa é a ameaça terrorista.

<b>General Loureiro dos Santos</b>	<b>Alemanha<sup>1</sup></b>	<b>Pedro Simões<sup>2</sup></b>	<b>CEDN</b>
Terrorismo Transnacional.	Extremismo e terrorismo internacional.	Terrorismo (usando Portugal como plataforma para o desenvolvimento das suas actividades).	Terrorismo transnacional.
Proliferação de fundamentalismos.			
A proliferação das ADM.	Proliferação de ADM.	Redes de comércio internacional de armas e material radioactivo .	Proliferação de ADM.
Crescimento populacional.		Vulnerabilização do sistema económico e do tecido produtivo por investimentos indesejáveis.	
Concentração nas megalópolis e desintegração social e étnica.		Grupos de jovens extremistas	
		Gangs de jovens delinquentes, devido à exclusão social, desemprego ou discriminação racial.	
		Novas seitas e movimentos pseudo-religiosos.	
Narcotráfico.		Redes transnacionais de imigração clandestina e	Crime organizado

<sup>1</sup> Traduzido de Defence Policy Guidelines, Aprovado pelo Ministro Federal da Defesa da RFA, a 21 de Maio de 2003. Disponível em <http://eng.bmvg.de/sicherheit/grundlagen/vpr.php>.

<sup>2</sup> Cf. Op. Cit., SIMÕES, 2002, 234 e 235.

		tráfico de seres humanos e o consumo e tráfico de drogas.	transnacional incluindo o tráfico de droga e as redes de promoção de imigração ilegal e tráfico de pessoas.
As grandes tensões económicas e as especulações financeiras e a predominância do modelo de mercado e a ameaça do fundamentalismo de mercado.		Utilização do sistema financeiro para branqueamento de capitais.	
		Internacionalização das organizações criminosas	
	Disrupção nos sistemas de informação e comunicação.	Cyber-crimes	
Acidentes ecológicos.		Prática de crimes ecológicos de grandes dimensões.	Atentados ao ecossistema, incluindo a poluição marítima, utilização abusiva de recursos marinhos e a destruição florestal.

### **Apêndice 3 – Avaliação por assuntos ou ligações dos atentados de 11 de Setembro.**

Adaptado de DeRosa, pp. 6 e ss e de Zoë Baird et al. p.28

Uma avaliação dos acontecimentos de 11 de Setembro fornece um exemplo de como a análise simples, por assuntos ou ligações poderia ser usada eficazmente para ajudar as investigações ou a análise dos planos dos terroristas. Usando a informação da lista de vigilância do governo, os registos de reservas da linha aérea, e dados agregados de registo público, a análise das ligações poderia ter identificado todos os 19 terroristas – para investigação mais detalhada – antes de 11 de Setembro. As ligações podem ser sumariadas como se segue:

#### **Ligações directas – Da Lista de vigilância**

- **Khalid Almihdhar** e **Nawaf Alhazmi**, ambos terroristas do voo 77 da *American Airlines* (AA), que se despenhou no Pentágono, faziam parte de uma lista de vigilância do governo dos EUA Ambos usaram os seus nomes reais na reserva dos voos.
- **Ahmed Alghamdi**, que desviou o voo 175 da *United Airlines* (UA), que se despenhou contra a torre sul do *World Trade Center*, fazia parte de uma lista de vigilância dos serviços de emigração, (*Immigration and Naturalization Service* (INS)), devido ao uso de vistos já expirados. Usou o seu nome real para reservar o voo.

#### **Análise de ligações – Um grau de separação**

- Dois outros terroristas usaram o endereço de contacto do Khalid Almihdhar, para a reserva dos seus voos. Foram o Mohamed Atta, que desviou o voo 11 da AA, que se despenhou contra a torre norte do World Trade Center, e Marwan Al Shehhi, que desviou o voo 175 da UA.
- Salem Alhazmi, que desviou o voo 77 da AA, usou o mesmo endereço de contacto, na sua reserva, que o Nawaf Alhazmi.
- O número de passageiro frequente que Khalid Almihdhar usou, para fazer a sua reserva, foi também usado pelo terrorista **Majed Moqed** para fazer a sua reserva no voo 77 da AA.
- **Hamza Alghamdi**, que desviou o voo 175 da UA 175, usou o mesmo endereço de contacto, para efectuar a sua reserva, que o Ahmed Alghamdi.

- **Hani Hanjour**, que desviou o voo 77 da AA, vivia com Nawaf Alhazmi and Khalid Almihdhar, um facto que pesquisas em registos públicos poderia ser encontrado.

#### **Análise de ligações – Dois graus de separação**

- Mohamed Atta, já ligado a Khalid Almihdhar, usou, na sua reserva, o mesmo número de telefone para contacto que foi também usado por **Waleed Alshehri**, **Wail Alshehri**, e **Abdulaziz Alomari**, todos do voo 11 da AA, e por **Fayez Ahmed** e **Mohand Alshehri**, ambos do voo 175 da UA.
- Registos mostram que Hamza Alghamdi vivia com **Saeed Alghamdi**, **Ahmed Al Haznawi**, e **Ahmed Alnami**, todos terroristas do voo 93 da UA, que se despenhou na Pennsylvania.

#### **Análise de ligações – Três graus de separação**

- Wail Alshehri foi companheiro de quarto e partilhou apartado de correio com Satam **Al Suqami**, um terrorista do voo 11 da AA. Ahmed Al Haznawi vivia com **Ziad Jarrah**, um terrorista do voo 93 da UA

Assim, se o governo tivesse começado com dados da lista de vigilância e seguido as ligações seria possível que, pelo menos, todos os terroristas fossem identificados para posteriores investigações. Claro que neste exemplo não se incluem os falsos positivos – nomes de pessoas que não tinham ligações com os ataques, mas que estiveram em contacto e podiam ser ligados aos terroristas que se encontravam na lista de vigilância do governo.

## **Anexo A – Cópia do artigo do *The Observer* – Clima como maior ameaça**

Apresentamos a cópia do artigo publicado no Jornal britânico, 22 de Fevereiro de 2004, em que se afirma que o clima poderá ser uma enorme ameaça à população mundial.

“Mark Townsend and Paul Harris in New York  
Sunday February 22, 2004  
The Observer

Climate change over the next 20 years could result in a global catastrophe costing millions of lives in wars and natural disasters..

A secret report, suppressed by US defence chiefs and obtained by The Observer, warns that major European cities will be sunk beneath rising seas as Britain is plunged into a 'Siberian' climate by 2020. Nuclear conflict, mega-droughts, famine and widespread rioting will erupt across the world.

The document predicts that abrupt climate change could bring the planet to the edge of anarchy as countries develop a nuclear threat to defend and secure dwindling food, water and energy supplies. The threat to global stability vastly eclipses that of terrorism, say the few experts privy to its contents.

'Disruption and conflict will be endemic features of life,' concludes the Pentagon analysis. 'Once again, warfare would define human life.'

The findings will prove humiliating to the Bush administration, which has repeatedly denied that climate change even exists. Experts said that they will also make unsettling reading for a President who has insisted national defence is a priority.

The report was commissioned by influential Pentagon defence adviser Andrew Marshall, who has held considerable sway on US military thinking over the past three decades. He was the man behind a sweeping recent review aimed at transforming the American military under Defence Secretary Donald Rumsfeld.

Climate change 'should be elevated beyond a scientific debate to a US national security concern', say the authors, Peter Schwartz, CIA consultant and former head of planning at Royal Dutch/Shell Group, and Doug Randall of the California-based Global Business Network.

An imminent scenario of catastrophic climate change is 'plausible and would challenge United States national security in ways that should be considered immediately', they conclude. As early as next year widespread flooding by a rise in sea levels will create major upheaval for millions.

Last week the Bush administration came under heavy fire from a large body of respected scientists who claimed that it cherry-picked science to suit its policy agenda and suppressed studies that it did not like. Jeremy Symons, a former whistleblower at the Environmental Protection Agency (EPA), said that suppression of the report for four months was a further example of the White House trying to bury the threat of climate change.

Senior climatologists, however, believe that their verdicts could prove the catalyst in forcing Bush to accept climate change as a real and happening phenomenon. They also hope it will convince the United States to sign up to global treaties to reduce the rate of climatic change.

A group of eminent UK scientists recently visited the White House to voice their fears over global warming, part of an intensifying drive to get the US to treat the issue seriously. Sources have told The Observer that American officials appeared extremely sensitive about the issue when faced with complaints that America's public stance appeared increasingly out of touch.

One even alleged that the White House had written to complain about some of the comments attributed to Professor Sir David King, Tony Blair's chief scientific adviser, after he branded the President's position on the issue as indefensible.

Among those scientists present at the White House talks were Professor John Schellnhuber, former chief environmental adviser to the German government and head of the UK's leading group of climate scientists at the Tyndall Centre for Climate Change Research. He said that the Pentagon's internal fears should prove the 'tipping point' in persuading Bush to accept climatic change.

Sir John Houghton, former chief executive of the Meteorological Office - and the first senior figure to liken the threat of climate change to that of terrorism - said: 'If the Pentagon is sending out that sort of message, then this is an important document indeed.'

Bob Watson, chief scientist for the World Bank and former chair of the Intergovernmental Panel on Climate Change, added that the Pentagon's dire warnings could no longer be ignored.

'Can Bush ignore the Pentagon? It's going to be hard to blow off this sort of document. It's hugely embarrassing. After all, Bush's single highest priority is national defence. The Pentagon is no wacko, liberal group, generally speaking it is conservative. If climate change is a threat to national security and the economy, then he has to act. There are two groups the Bush Administration tend to listen to, the oil lobby and the Pentagon,' added Watson.

'You've got a President who says global warming is a hoax, and across the Potomac river you've got a Pentagon preparing for climate wars. It's pretty scary when Bush starts to ignore his own government on this issue,' said Rob Gueterbock of Greenpeace. Already, according to Randall and Schwartz, the planet is carrying a higher population than it can sustain. By 2020 'catastrophic' shortages of water and energy supply will become increasingly harder to overcome, plunging the planet into war. They warn that 8,200 years ago climatic conditions brought widespread crop failure, famine, disease and mass migration of populations that could soon be repeated.

Randall told The Observer that the potential ramifications of rapid climate change would create global chaos. 'This is depressing stuff,' he said. 'It is a national security threat that is unique because there is no enemy to point your guns at and we have no control over the threat.'

Randall added that it was already possibly too late to prevent a disaster happening. 'We don't know exactly where we are in the process. It could start tomorrow and we would not know for another five years,' he said.

'The consequences for some nations of the climate change are unbelievable. It seems obvious that cutting the use of fossil fuels would be worthwhile.'

So dramatic are the report's scenarios, Watson said, that they may prove vital in the US elections. Democratic frontrunner John Kerry is known to accept climate change as a real problem. Scientists disillusioned with Bush's stance are threatening to make sure Kerry uses the Pentagon report in his campaign.

The fact that Marshall is behind its scathing findings will aid Kerry's cause. Marshall, 82, is a Pentagon legend who heads a secretive think-tank dedicated to weighing risks to

national security called the Office of Net Assessment. Dubbed 'Yoda' by Pentagon insiders who respect his vast experience, he is credited with being behind the Department of Defence's push on ballistic-missile defence.

Symons, who left the EPA in protest at political interference, said that the suppression of the report was a further instance of the White House trying to bury evidence of climate change. 'It is yet another example of why this government should stop burying its head in the sand on this issue.'

Symons said the Bush administration's close links to high-powered energy and oil companies was vital in understanding why climate change was received sceptically in the Oval Office. 'This administration is ignoring the evidence in order to placate a handful of large energy and oil companies,' he added."

## **Anexo B – Modelo proposto pelo Coronel Carlos Chaves para o Sistema de Informações da República.**

### **1 – Para o Sistema de Informações da República**

Assente na existência de uma «comunidade de informações» e, estabelecido o sistema organizacional em «rede», o SIR seria constituído por (ver adenda A):

- Dois serviços de informações – SIS e SIE;
- Direcções-Gerais, Departamentos e Células de Informações nos Ministérios, e outros Serviços do Estado que contribuam para o estabelecimento e prossecução da Política de Defesa Nacional;
- **Órgãos de fiscalização externa**, a constituir de acordo com os objectivos próprios, junto da Assembleia da República, Conselho Superior de Magistratura e Conselho Superior do Ministério Público (Procuradoria-Geral da República);
- **Órgão superior de segurança** a estabelecer em intima ligação com o Gabinete Nacional de Segurança (GNS) / Autoridade Nacional de Segurança (ANS);
- Direcção superior do sistema atribuída à **competência própria** do Primeiro-Ministro (PM), dispondo para tal de **um órgão executivo de coordenação e direcção** – o Gabinete Coordenador do Sistema de Informações da República (GCSIR) – a funcionar na directa dependência do PM ou integrando a Presidência do Conselho de Ministros. O GCSIR seria ainda responsável pela elaboração das sínteses de informações para as mais altas autoridades do Estado, bem como pelas notas de antecipação e alerta;
- Uma Escola Nacional de Informações (ENI).

Como funcionamento geral do sistema, preconizamos:

- **As nomeações** do Director do GCSIR, dos Directores dos Serviços (SIS e SIE), e da ENI, seria feita por Decreto do PR, sobre proposta do PM, com base em Resolução do Conselho de Ministros (CM), e após audição das entidades propostas por uma comissão competente e especializada da AR. Esta comissão produziria um parecer objectivo sobre possíveis objecções e/ou limitações, com carácter secreto, a ser submetido à consideração do Governo;

- **Os objectivos anuais** para o SIR seriam fixados pelo CSDN, sobre proposta do PM;
- **A directiva anual** de funcionamento do SIR seria elaborada pelo CSSIR<sup>3</sup>, sob proposta do Director do GCSIR, e aprovada pelo CM;
- **O plano anual de actividades** do SIR seria elaborado pelo CESIR<sup>4</sup> e aprovado pelo PM;
- Ser garantida a **mobilidade do pessoal** do sistema pelos serviços, direcções, departamentos e células sempre que as missões/objectivos o justifiquem e, sob decisão do Director do GCSIR;

Considerando o sistema organizativo proposto (em rede), parece-nos útil reflectir sobre a experiência obtida nas décadas de 70 e 80 do século passado com os Centros Locais de Coordenação de Informações (CLCI), e que se estude a implementação de organismos semelhantes junto das unidades militares<sup>5</sup> e dos Comandos Militares Regionais<sup>6</sup>, inserindo-os na filosofia geral preconizada para o sistema.

---

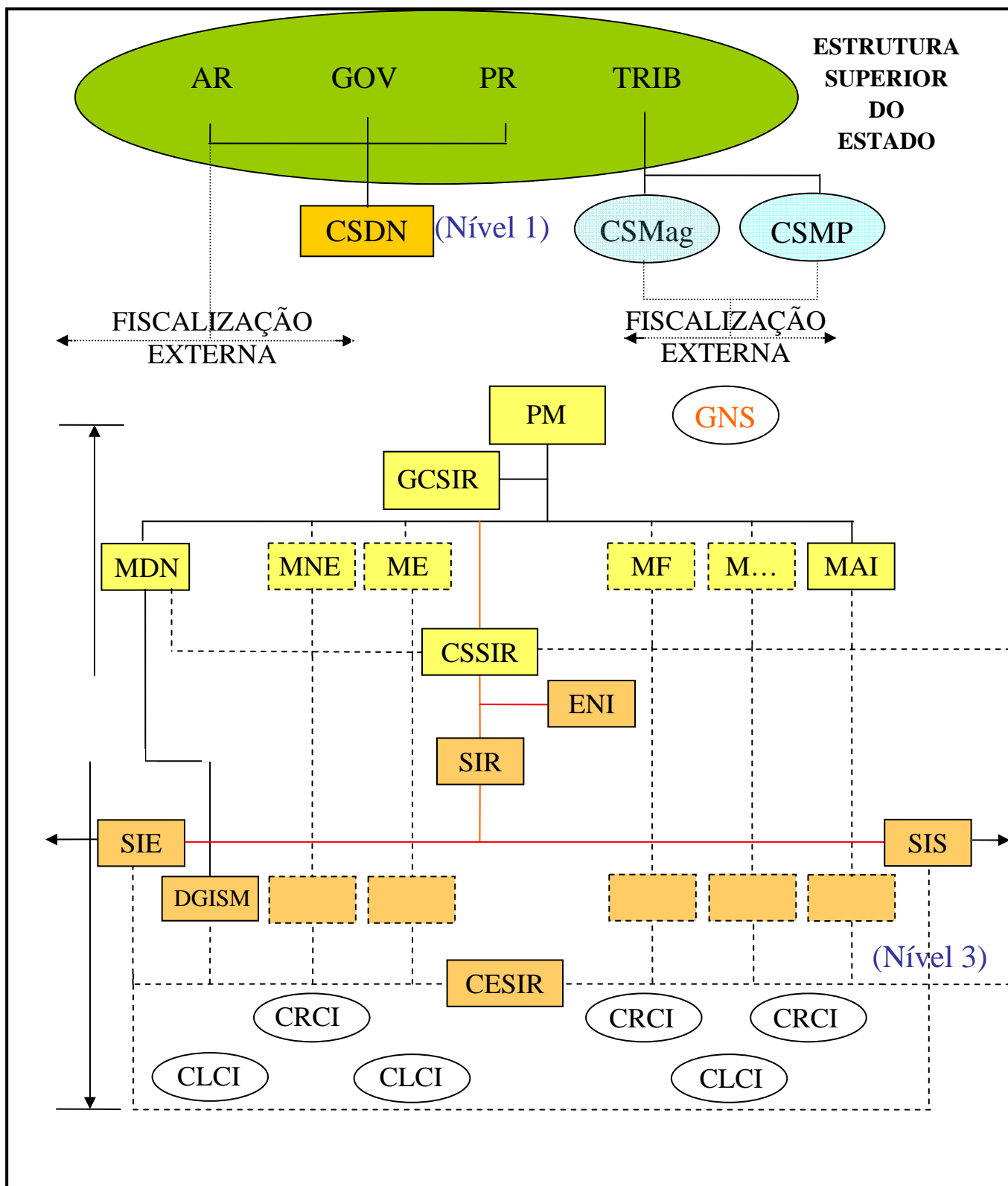
<sup>3</sup> Em Adenda B propomos a constituição do CSSIR;

<sup>4</sup> Em Adenda C propomos a constituição do CESIR;

<sup>5</sup> Os CLCI.

<sup>6</sup> Os organismos a implementar junto dos Comandos Militares Regionais chamar-se-iam Centros Regionais de Coordenação de Informações (CRCI).

Adenda A – Modelo do Sistema de Informações da República



**Adenda B – Proposta de Constituição do Conselho Superior do Sistema de Informações da República (CSSIR)**

**Presidente** - Primeiro-Ministro.

**Membros** - Ministros das Pastas que concorrem para a preparação e execução da Política da Defesa Nacional:

- Ministro da Defesa Nacional (MDN);
- Ministro dos Negócios Estrangeiros (MNE);
- Ministro das Finanças (MF);
- Ministro da Economia (ME);
- Ministro das Obras Públicas, Transportes e Comunicações (MOPTC);
- Ministro da Administração Interna (MAI);
- Ministro da Justiça (MJ);
- Ministro da Cultura (MC);
- Outros (EV).

**Secretário** – Director do Gabinete Coordenador do Sistema de Informações da República.

**Apoio Administrativo** - Prestado pelo Gabinete Coordenador do Sistema de Informações da República.

**Adenda C: Proposta do Conselho Executivo do Sistema de Informações da República (CESIR)**

**Presidente** - Director do Gabinete Coordenador do Sistema de Informações da República.

**Membros** – Serão as seguintes Entidades:

- Secretário Geral do Gabinete Coordenador de Segurança (MAI);
- Director do Sistema de Informações e Segurança (SIS);
- Director do Serviço de Informações Estratégicas (SIE);
- Director da Direcção-Geral de Informações e Segurança Militar (DGISM/MDN);
- Responsáveis por outros Departamentos existentes ao nível dos Ministérios que concorram para a preparação e execução da Política de Defesa Nacional;
- Comandante-Geral da Guarda Nacional Republicana (GNR);
- Director Nacional da Polícia de Segurança Pública (PSP);
- Director-Geral do Serviço de Estrangeiro e Fronteiras (SEF);
- Director-Geral da Polícia Judiciária (PJ);
- Director Nacional do Serviço de Protecção Civil e Bombeiros (SNPCB).

**Secretário** – A nomear pelo Director do Gabinete Coordenador do Sistema de Informações da República, mas, sendo elemento pertencente ao mesmo.

**Apoio Administrativo** - Prestado pelo Gabinete Coordenador do Sistema de Informações da República.

## **Anexo C – k-ANONYMITY; um modelo de protecção da privacidade**

Anexamos o trabalho de Latanya Sweeney que tem sido empregue pelo DARPA para implementação de sistemas de salvaguarda da privacidade em projectos que empregam o *data mining*.